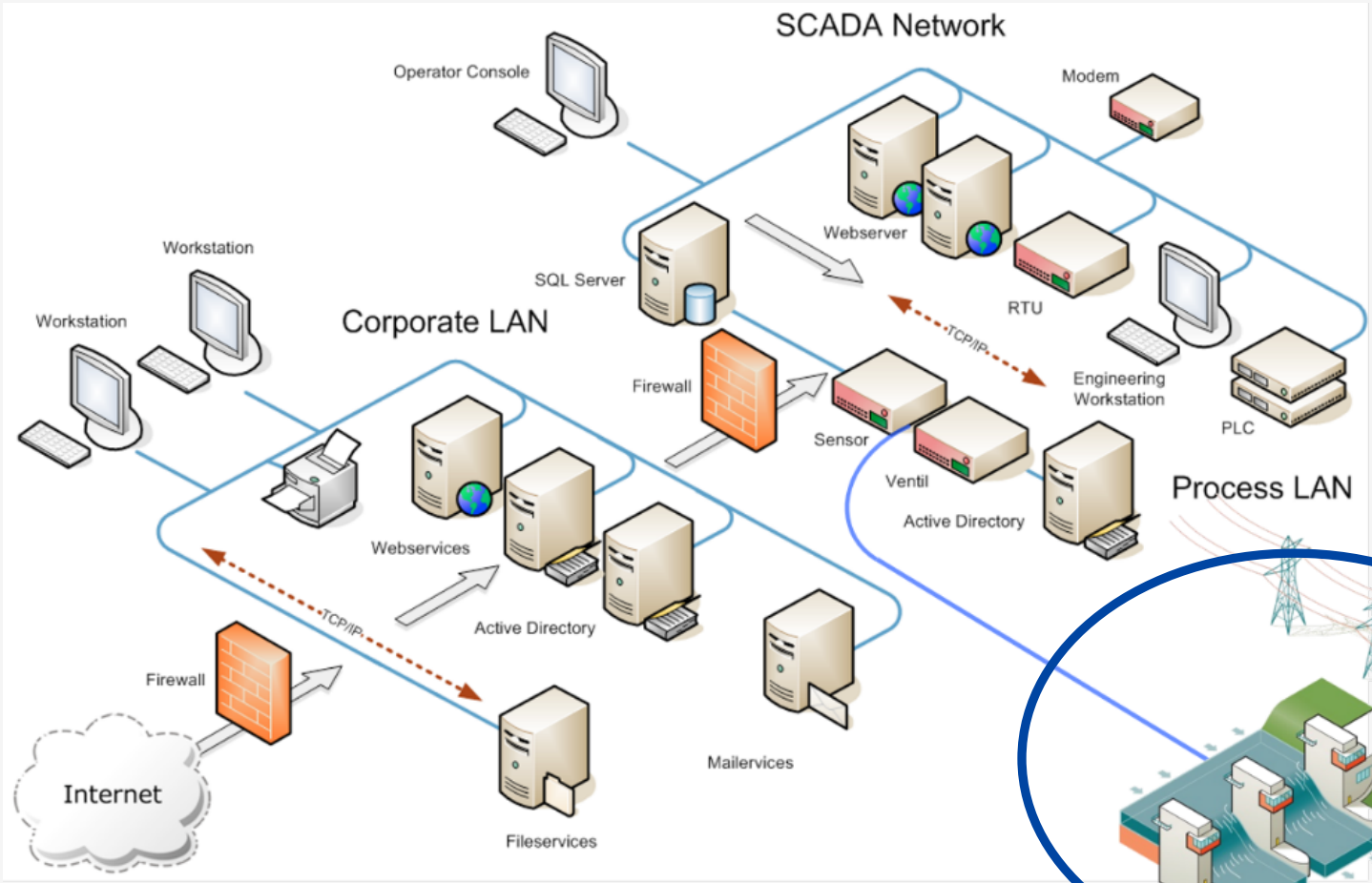
Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion

Marina Krotofil

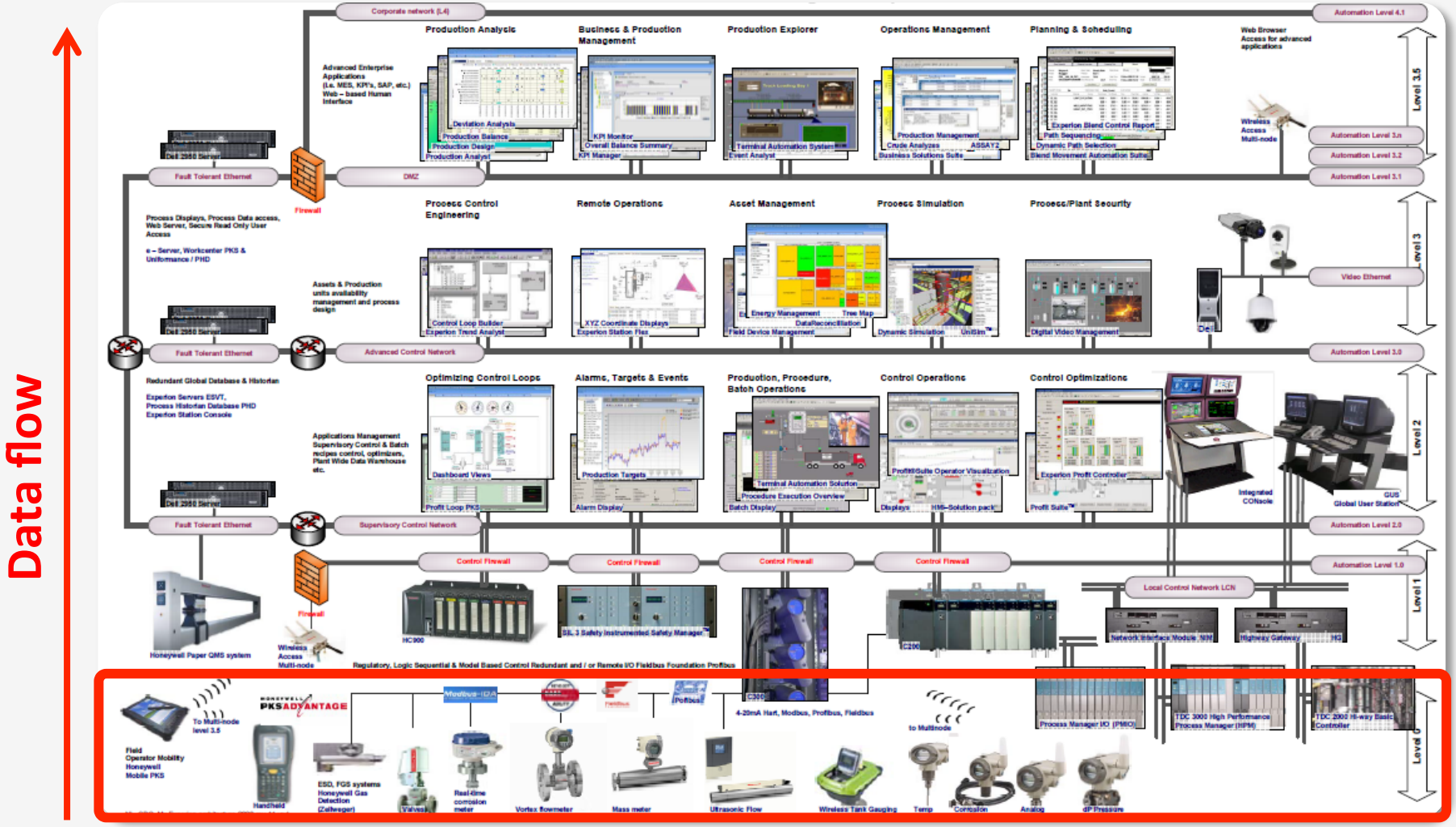
HITB Singapore
14.10.2015

Industrial Control Systems aka SCADA



Physical application

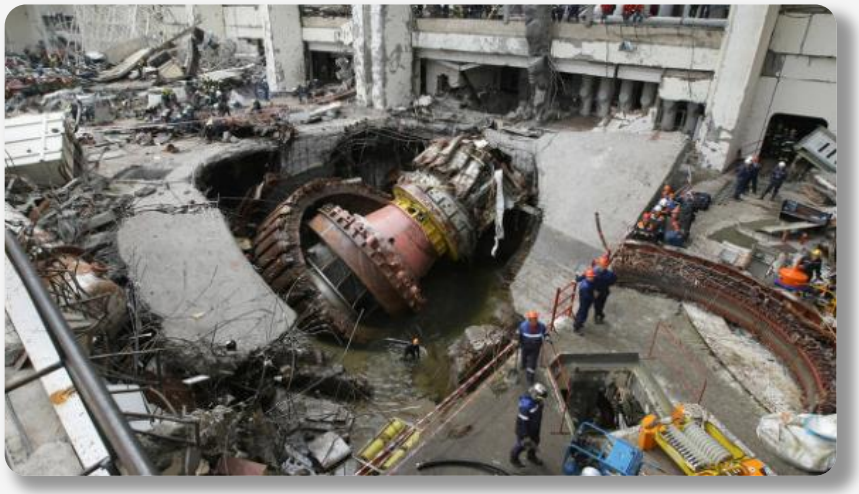
Industrial Control Systems aka SCADA



Cyber-physical systems

Cyber-physical systems are IT systems “embedded” in an application in the physical world

Interest of the attacker is in the physical world



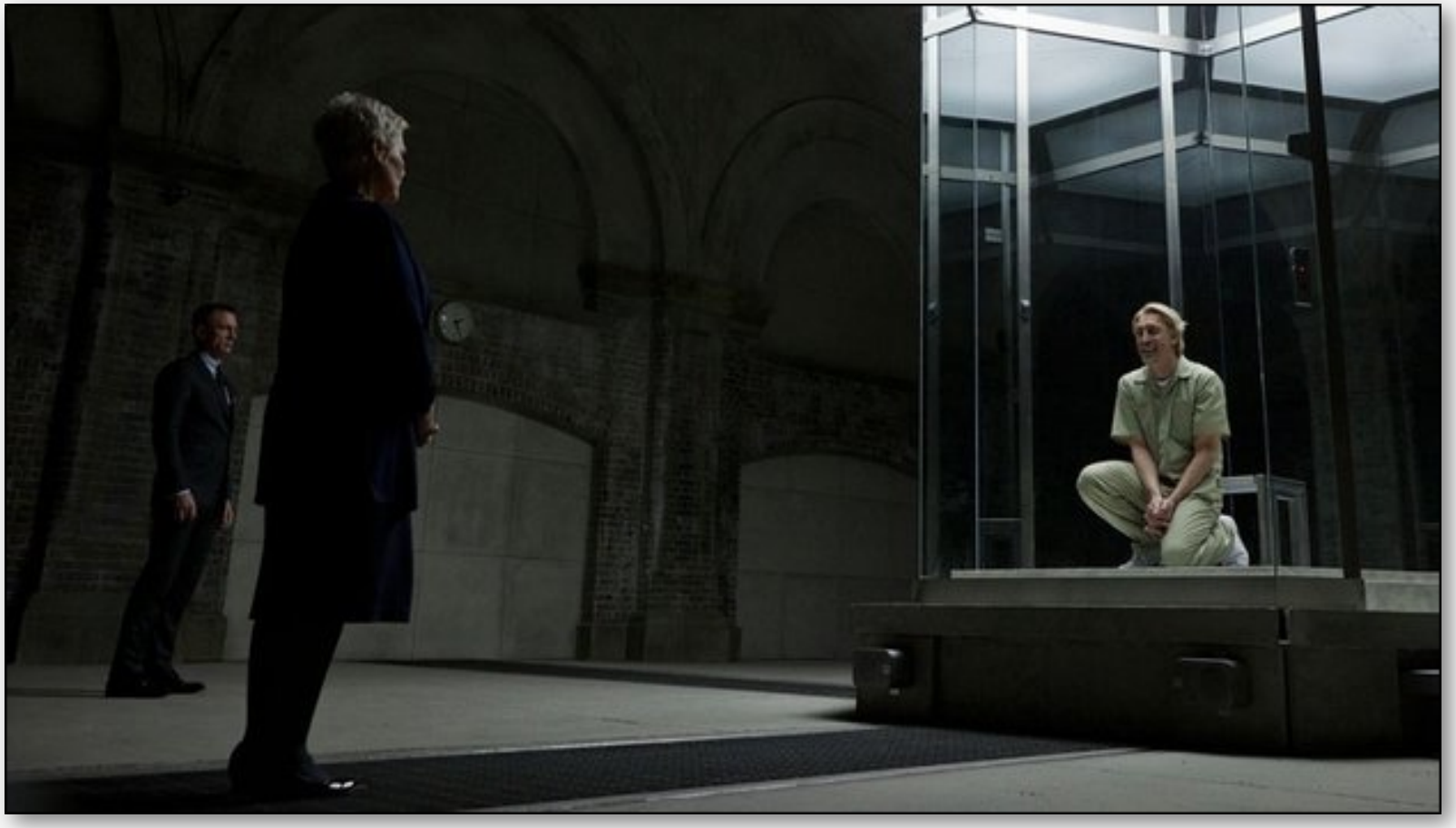
The world is not the same anymore

James Bond 007 –
Casino Royale

Pity!!

James Bond 007 – Skyfall

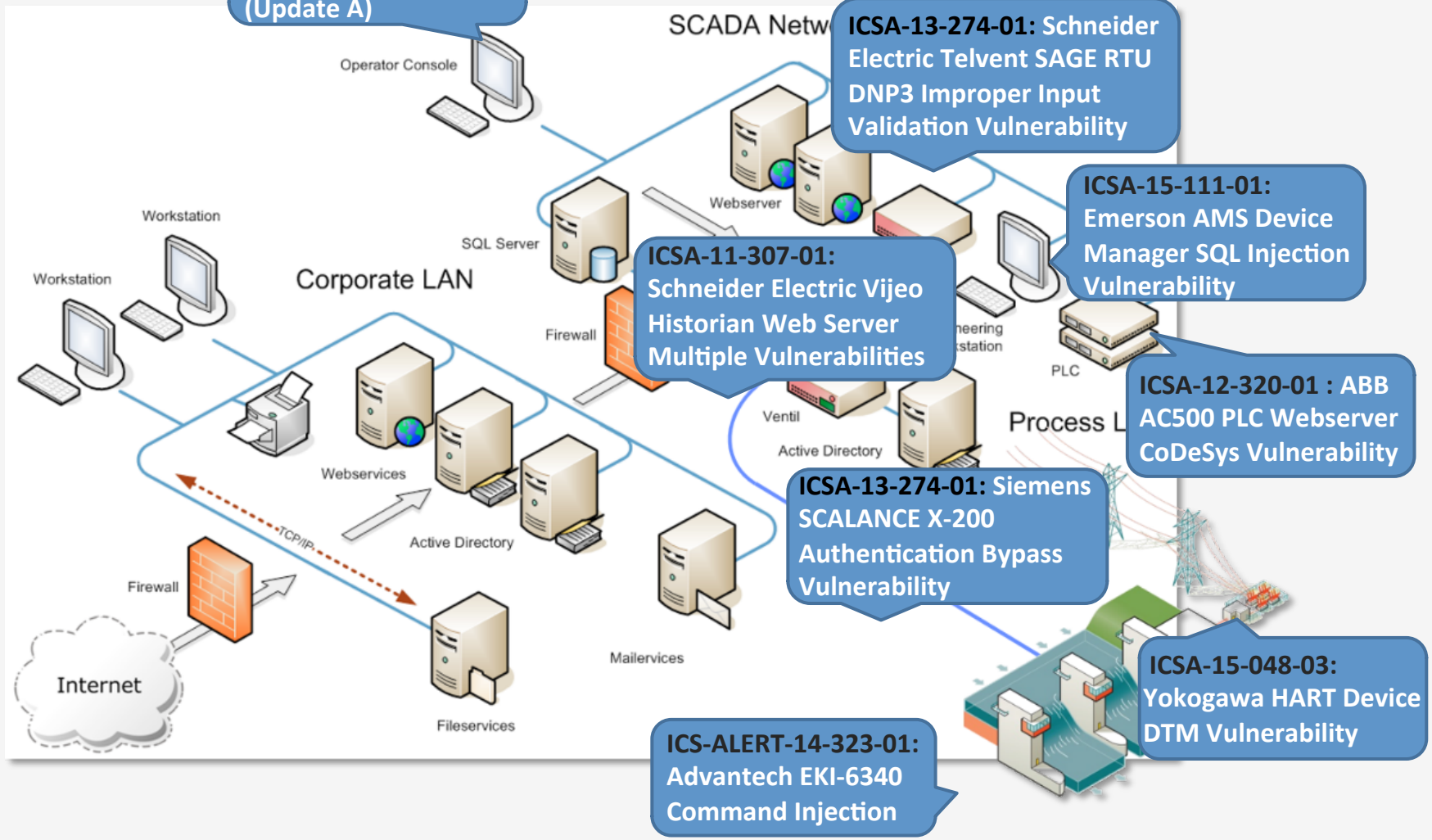
Cyber-physical hack



James Bond 007: Skyfall

Control systems security

Control equipment vulnerabilities



ICS-CERT recommendation

ICSA-13-274-01: Siemens SCALANCE X-200 Authentication Bypass Vulnerability

IMPACT

Successful exploitation of this vulnerability may allow attackers to perform administrative operations over the network without authentication.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

Typical idea about post exploitation

magic button
(does not exist!)

TCP/IP based communication

Industrial switch

Ethernet, my old friend
(hack meeee!!!)

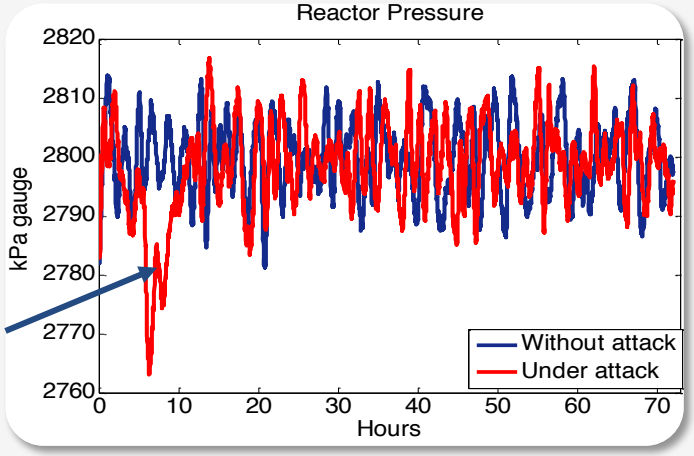
Modbus, DNP, IEC850 are common protocols

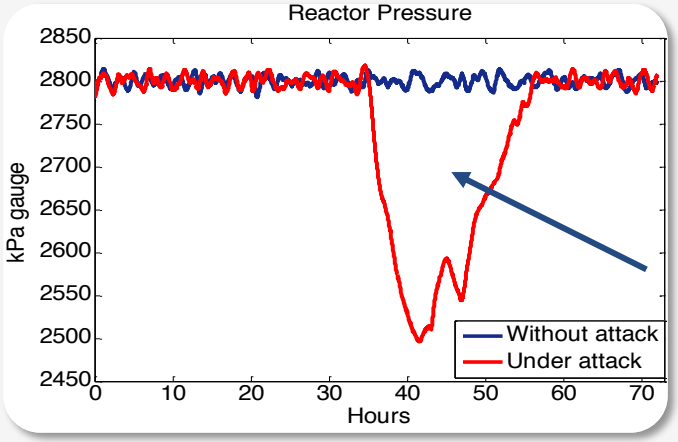
Hear is the plant. What is the plan?

Source: simentari.com

Timing of the DoS attack

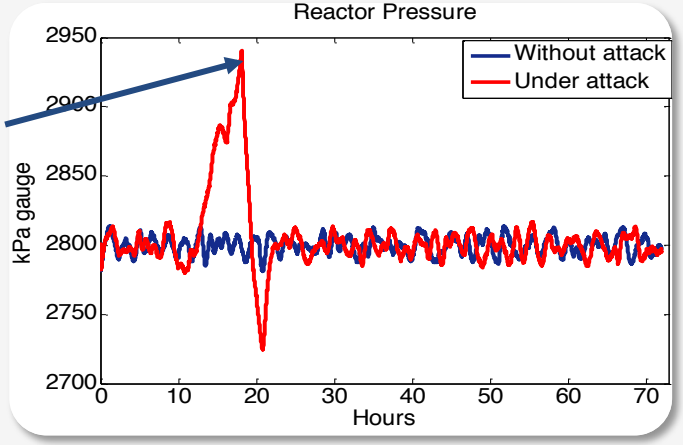
Ordinary glitch

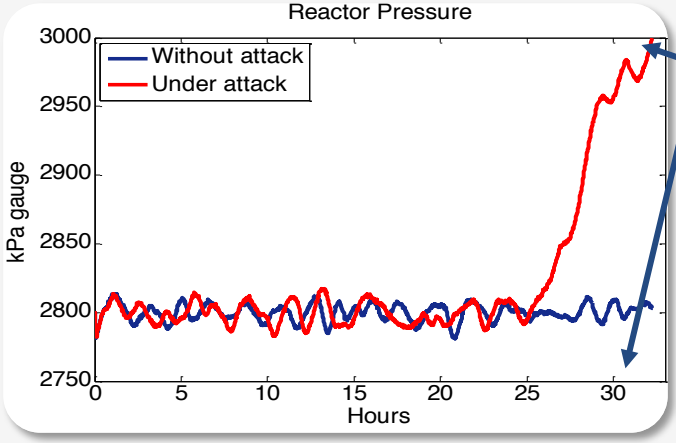




Economic inefficiency

Near miss (almost safety accident)





Safety shutdown

Impact of 8h long attack on reactor pressure at random time

Impact evaluation

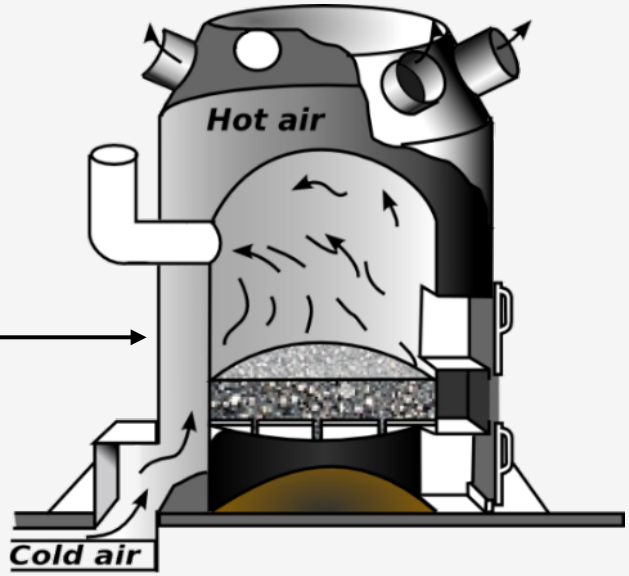
- What exactly the attacker can do with the vulnerability?
- Any further necessary conditions required?
- How severe the potential physical impact?

Answering these questions requires understanding how the attacker interacts with the control system and the process

Process control

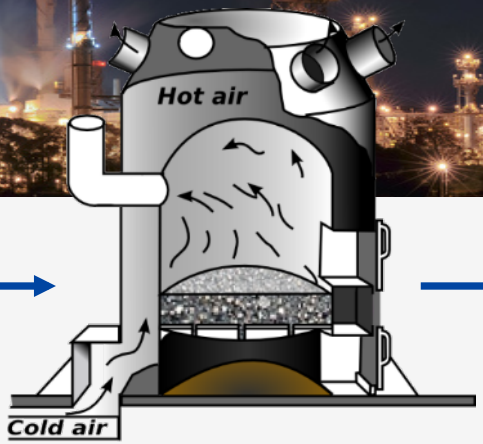
Process control automation

Set point



Running downstairs to turn on the furnace every time it gets cold is tiring, so you automate it with a thermostat

Control loop



Physical process

Actuators

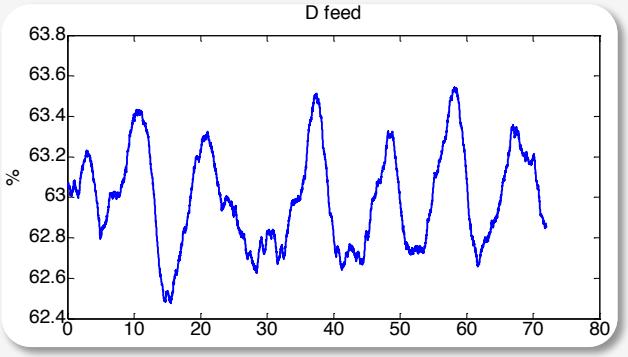
Sensors

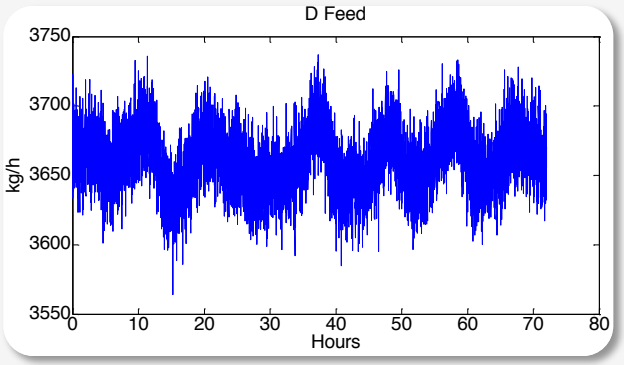
Adjust themselves to influence process behavior

Control system

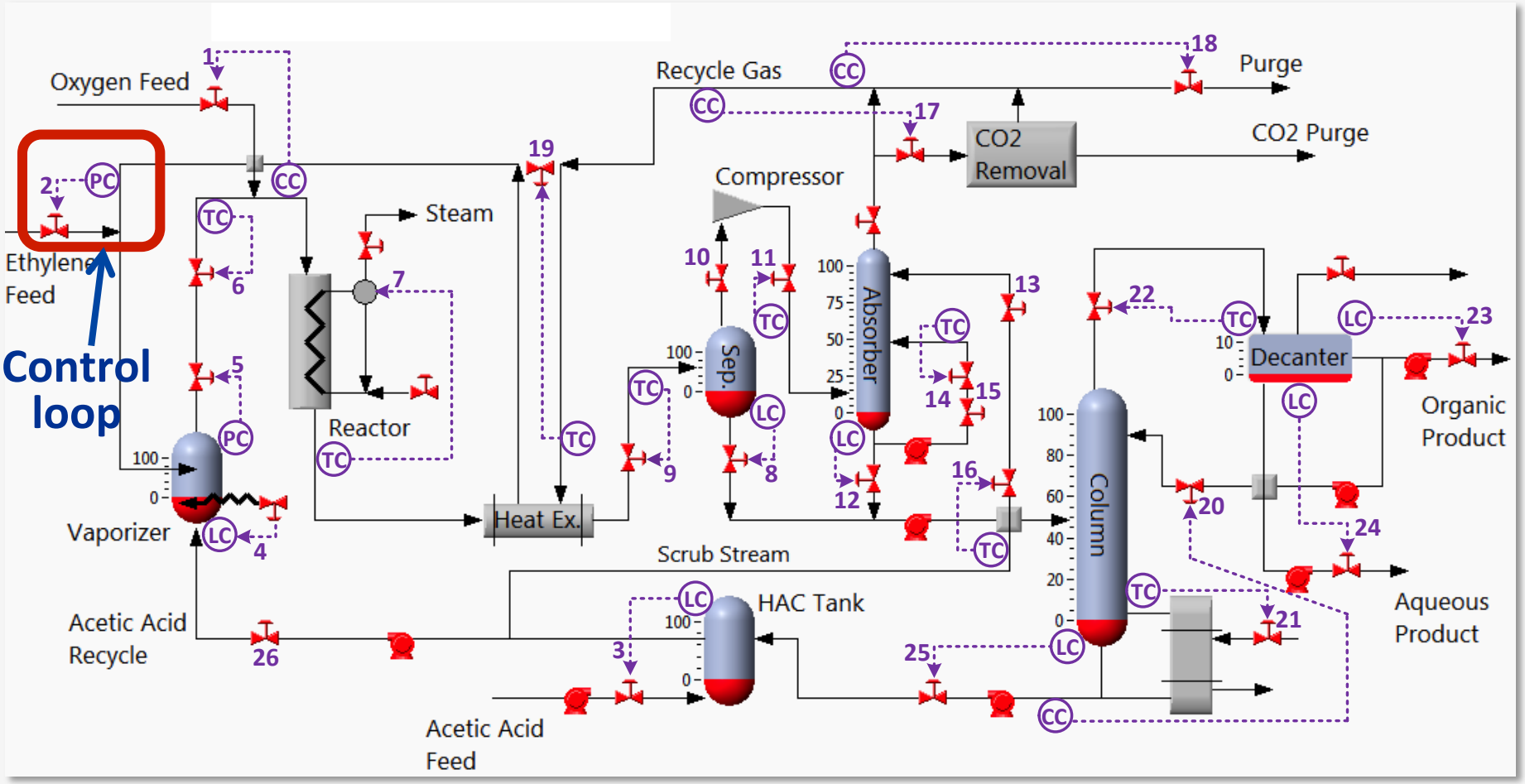
Measure process state

Computes control commands for actuators

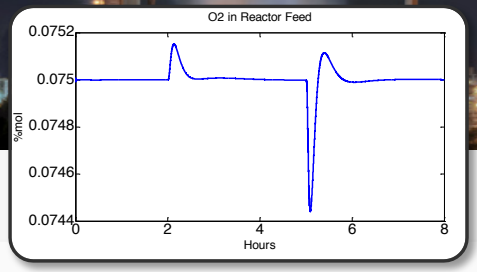


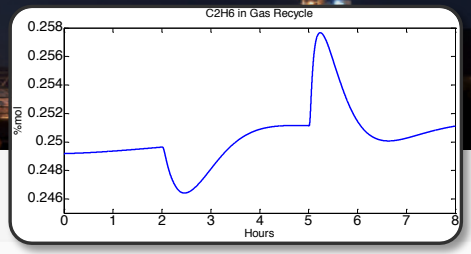


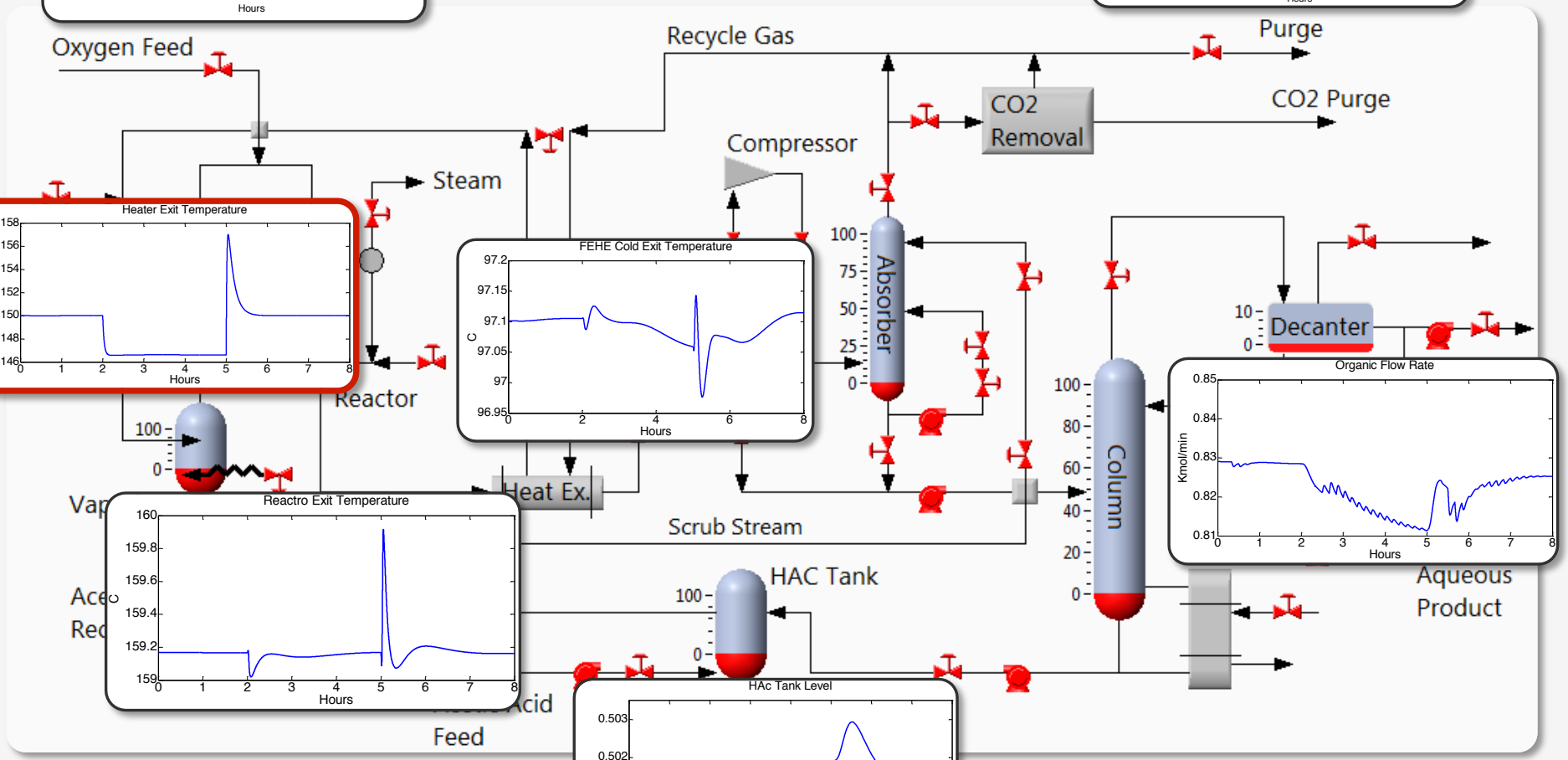
Understanding control structure



Process interdependencies



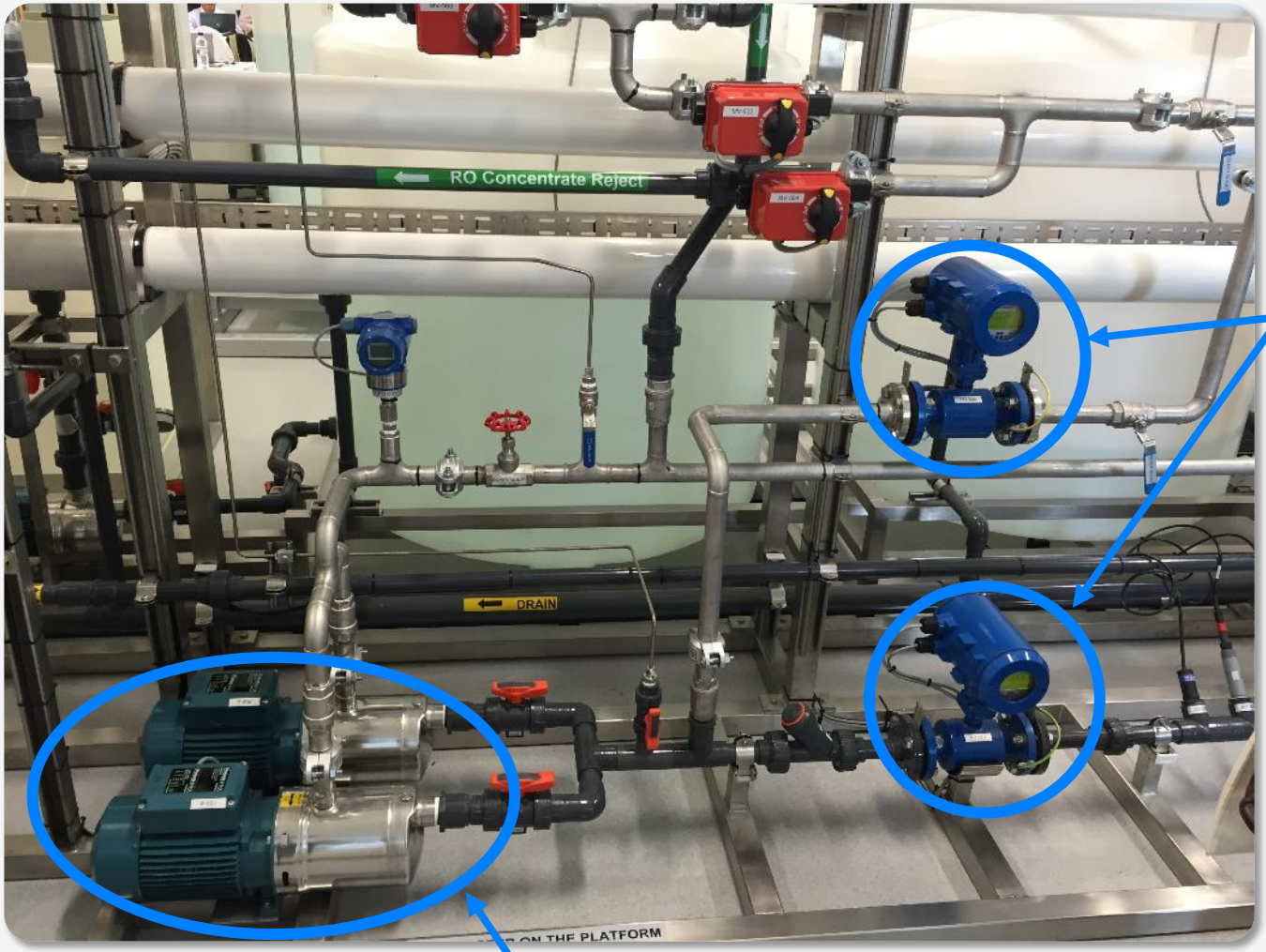




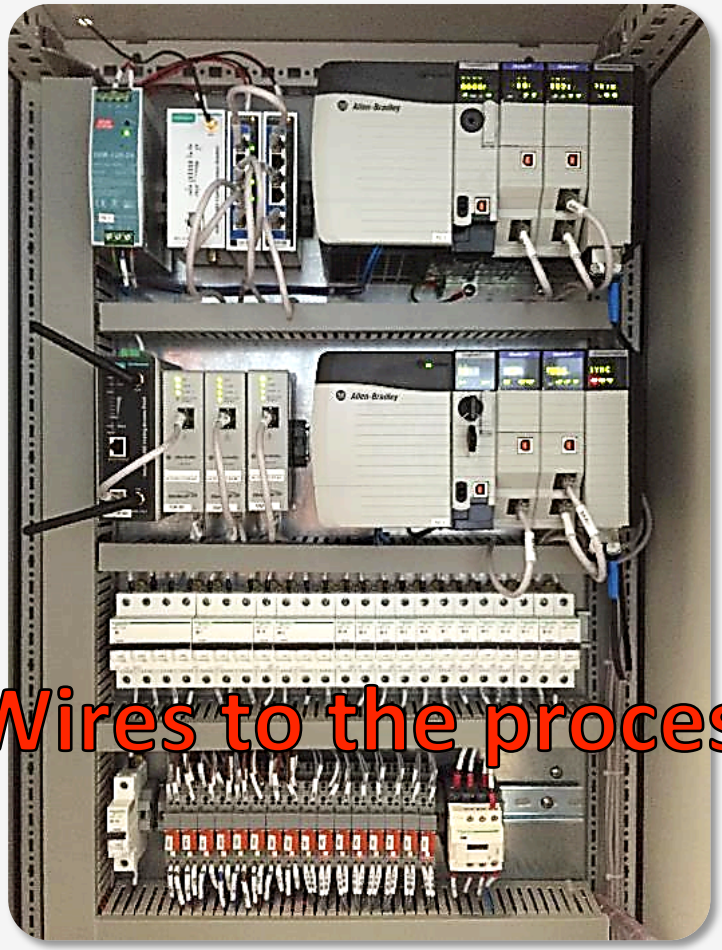
Control equipment

- In large –scale operations control logic gets more complex than a thermostat
- The control is typically done by a programmable logic controller (PLC)

Plant floor



Field communication



PLC

Wires to the process

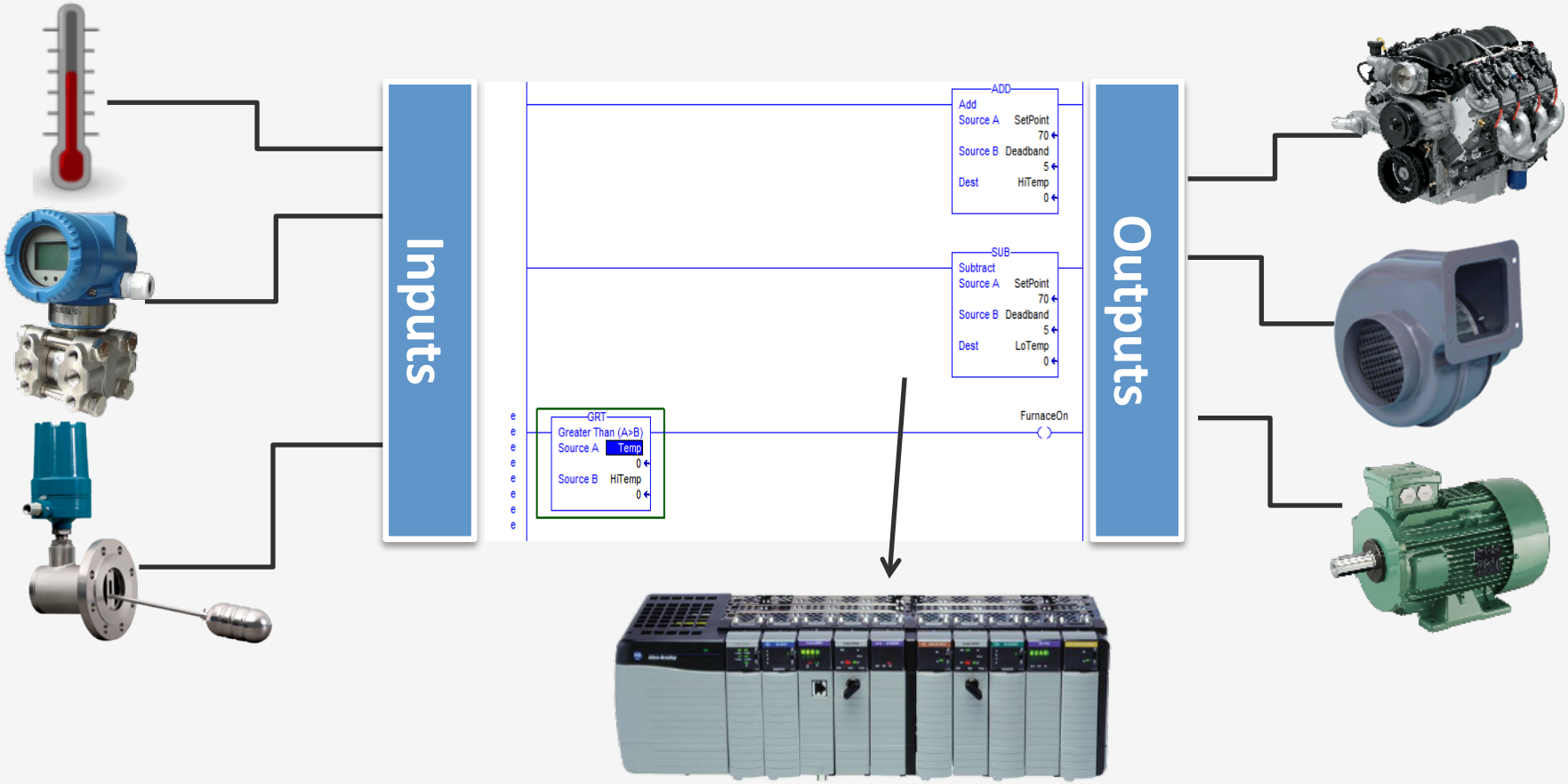
Wires are run from sensors and actuators into wiring cabinets

PLC internals

1. Copy data from inputs to temporary storage
2. Run the logic
3. Copy from temporary storage to outputs

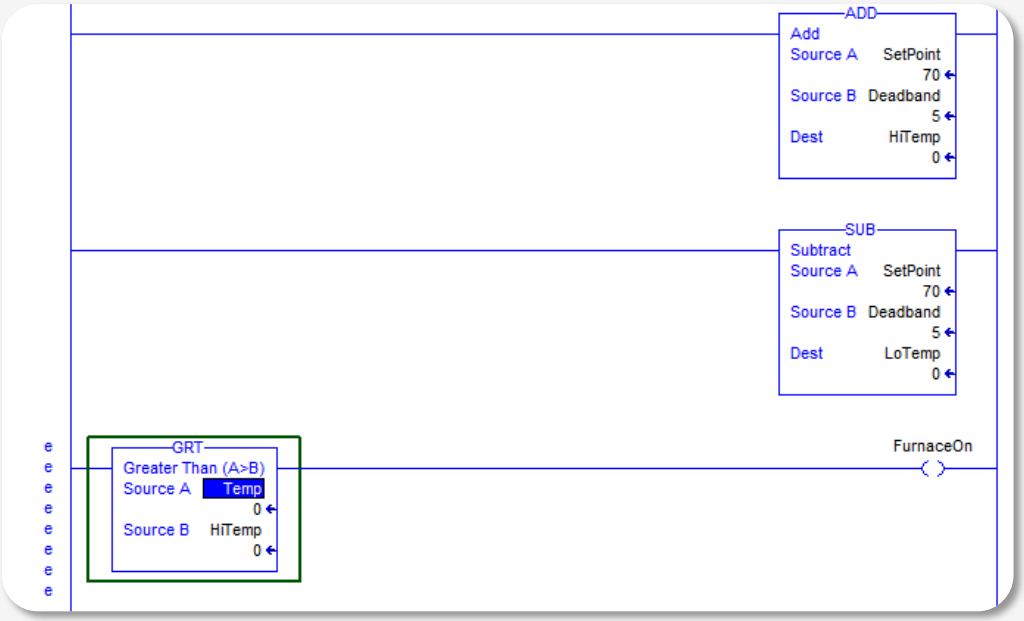
Sensors

Actuators



Control logic

- Defines what should (not) happen to the process: conditions, order, time



(Programmed graphically most of time. Nope, no python or java)

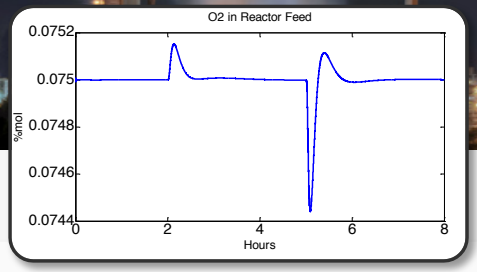
If tank pressure in PLC 1 > 1800 reduce inflow in PLC 3

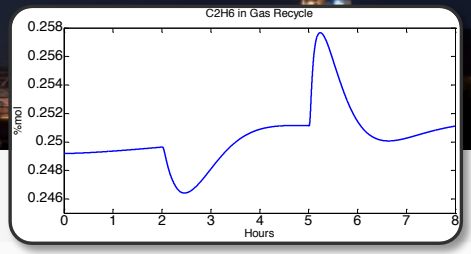
Interlocks

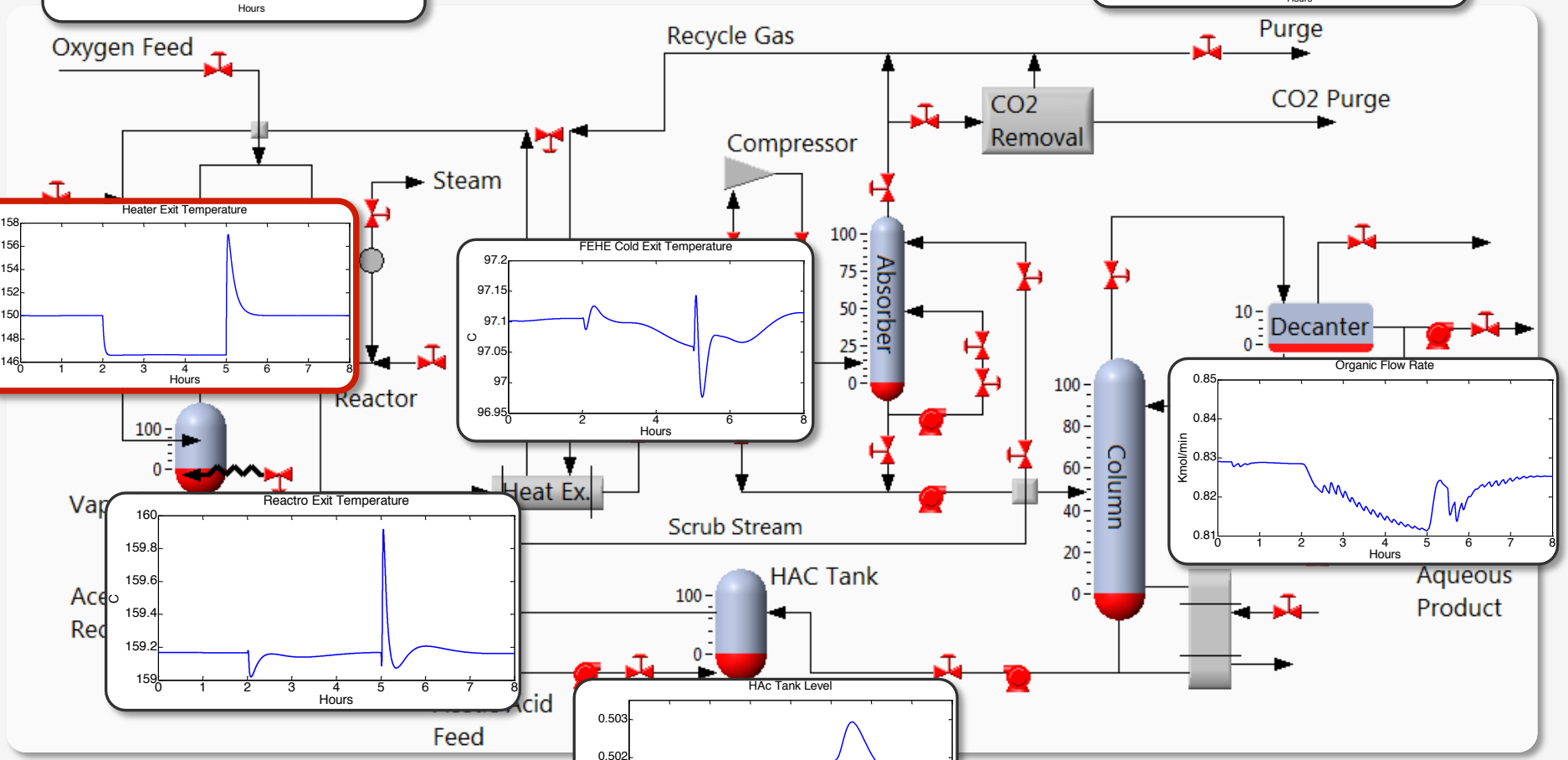
- Process safety increasingly depends on the logic in the controllers
- Ladder logic can tell you a lot about what the engineer that designed the process was worried about
- Search for the master stop

The motor should not be running when the valve is closed

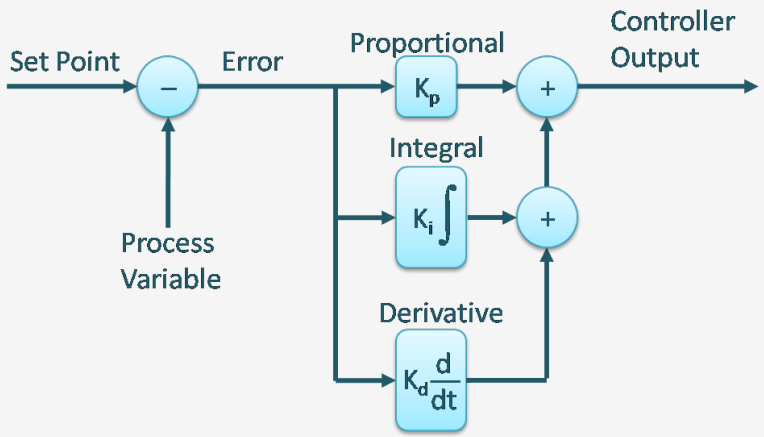
Process interdependencies

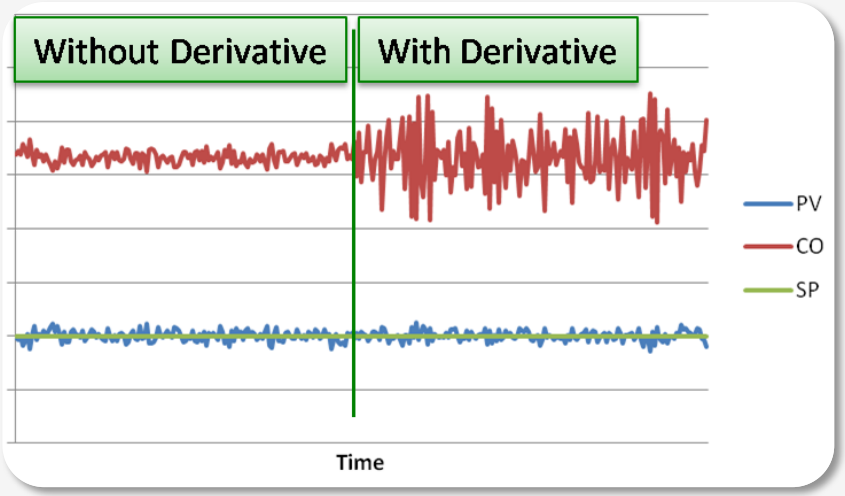






PID control



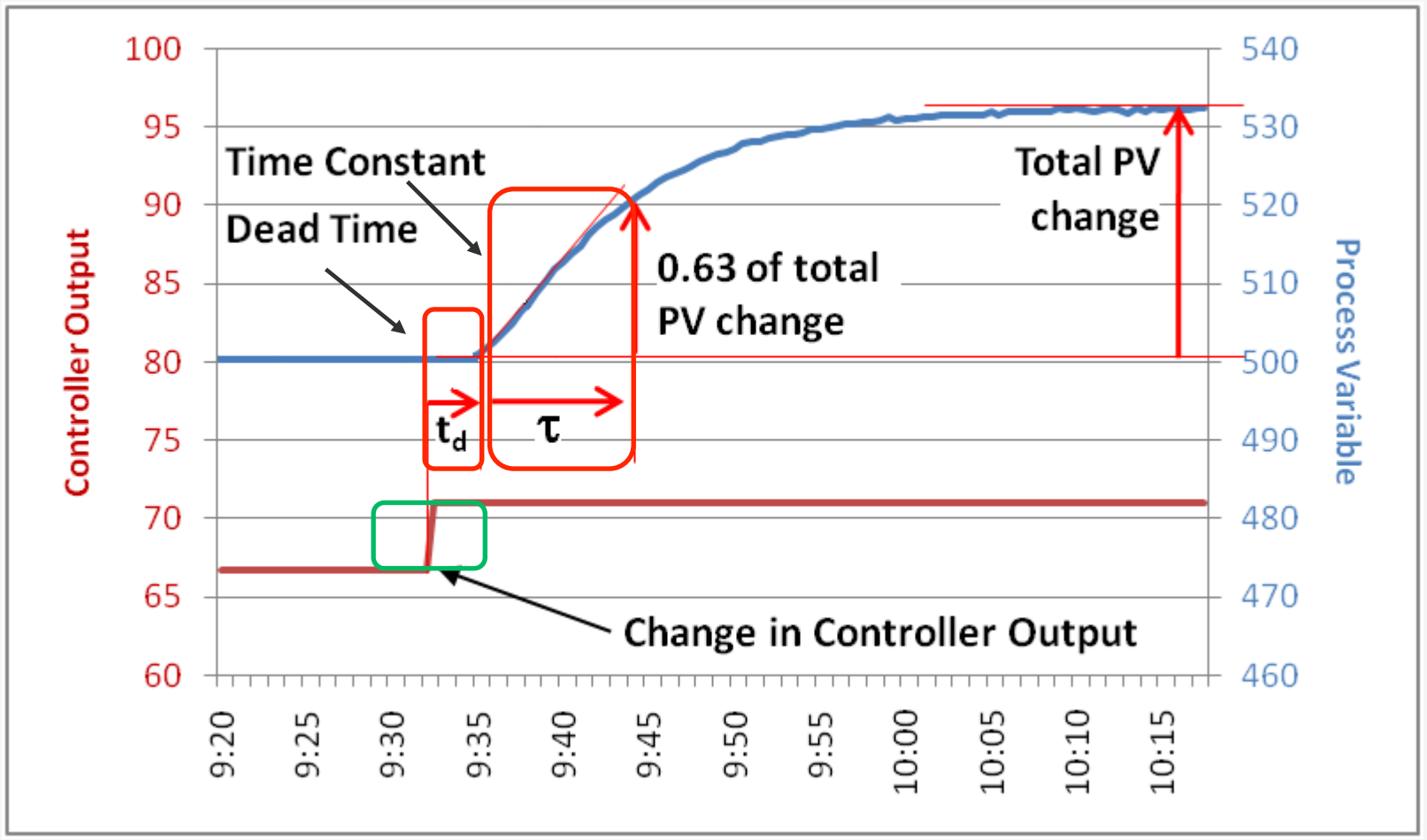


$$u(t) = K\left(e(t) + \frac{1}{T_i}\int_0^t e(\tau)d\tau + T_d\frac{de(t)}{dt}\right)$$

- **PID: proportional, integral, derivative –** most widely used control algorithm on the planet
- The sum of 3 components makes the final control signal
- PI controllers are most often used

Jacques Smuts „Process Control for Practitioners“

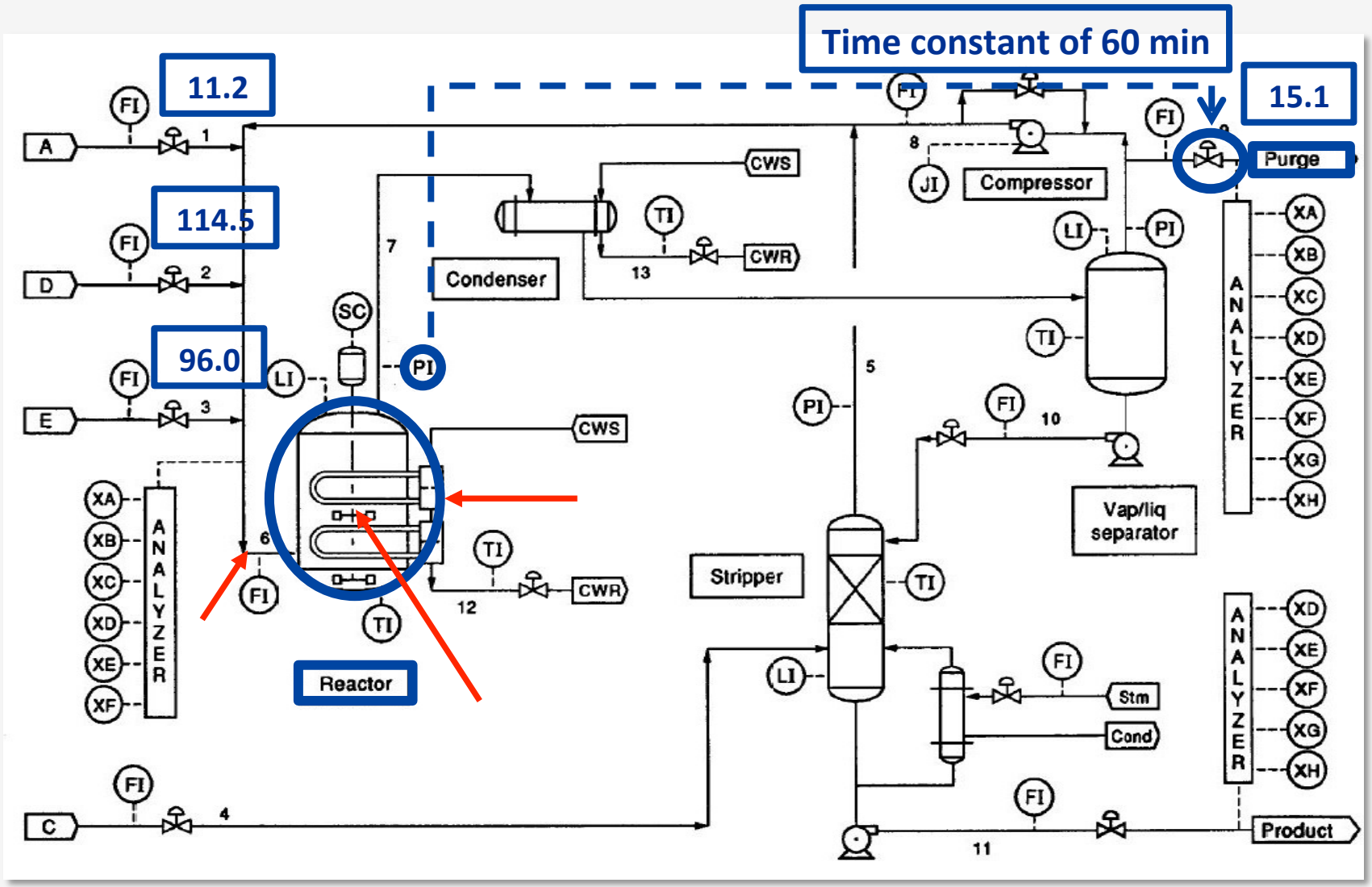
Time constants



Requires reconnaissance on live process

Jacques Smuts „Process Control for Practitioners“

Process control vulnerability



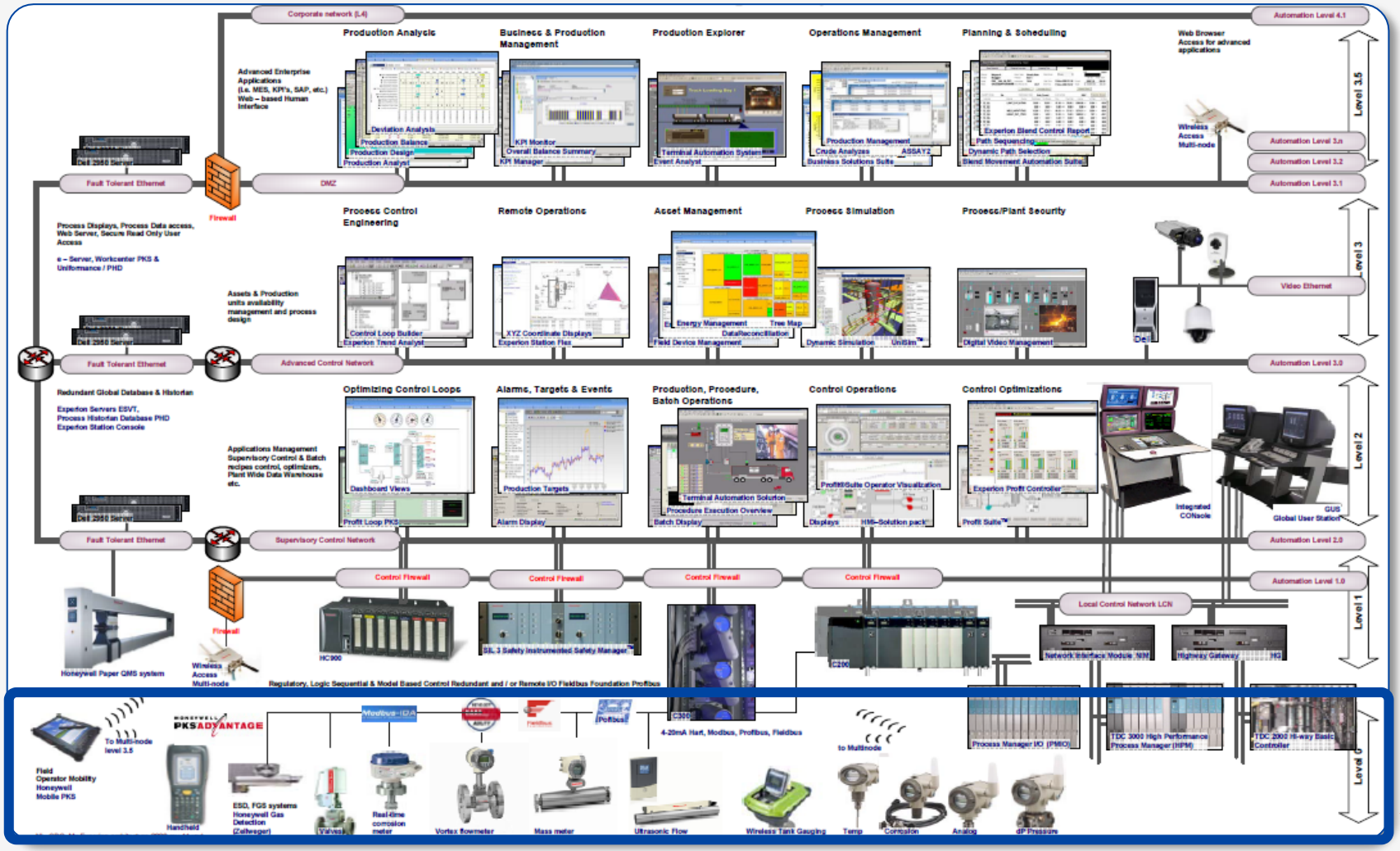
PLC cannot do it alone

- PLC does not have the complete picture and time trends
- Human operators watch the process 7/24
- **Most important task: resolving of alarms**

Operator is not almighty

Sanity checks

Industrial Control Systems aka SCADA



Definition of real time (time constant)

Physical process

Why to hack SCADA

Industry means big business
Big business == $$$$$$$

Why to attack ICS

Industry means big business
Big business == $$$$$$$

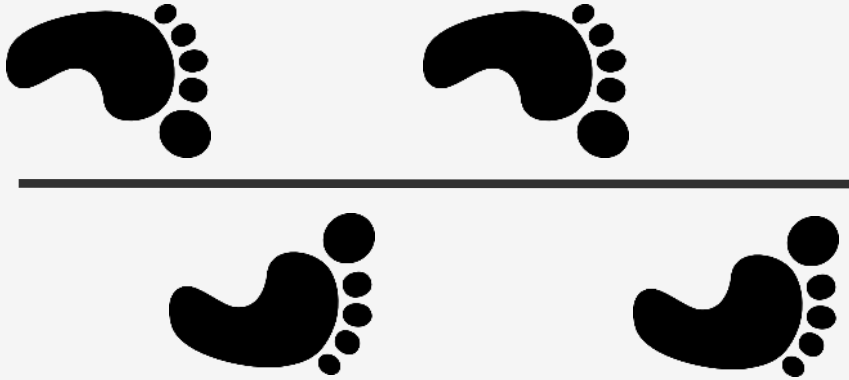
Alan Paller of SANS (2008):

In the past two years, hackers have successfully penetrated and extorted multiple utility companies that use SCADA systems.

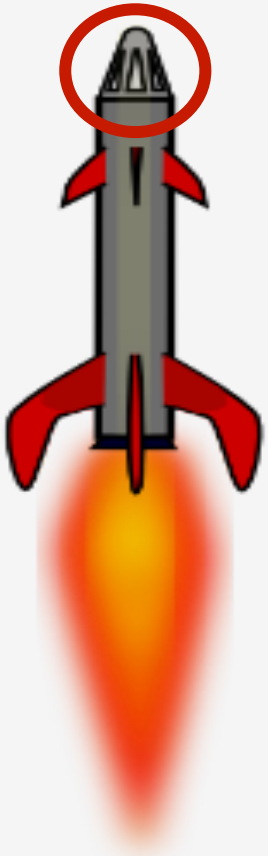
Hundreds of millions of dollars have been extorted, and possibly more. It's difficult to know, because they pay to keep it a secret. **This kind of extortion is the biggest untold story of the cybercrime industry.**

Attack payload

Attack objective



Cyber-physical payload



What can be done to the process

Equipment damage

- Equipment overstress
- Violation of safety limits

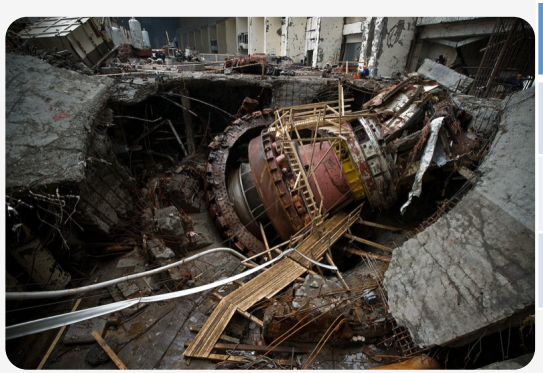
Production damage

- Product quality and product rate
- Operating costs
- Maintenance efforts

Compliance violation

- Safety
- Pollution
- Contractual agreements

Paracetamol



Purity	Relative price, EUR/kg
98%	1
99%	5
100%	8205

Source: http://www.sigmaaldrich.com/

Attack considerations

Equipment damage

Production damage

Compliance violation

- **Equipment damage**
  - Comes first into anybody's mind (+)
  - Irreversible (∓)
  - Unclear collateral damage (-)
  - May transform into compliance violation, e.g. if it kills human (-)
- **Compliance violation**
  - Must be reported to the authorities (∓)
  - Will be investigated by the responsible agencies (-)
  - Compliance regulations are public knowledge (+)
  - Unclear collateral damage (-)

Production damage attack

Attack goal: persistent economic damage

Get the party started!

Plants for sale

From LinkedIn

+Follow Tommy

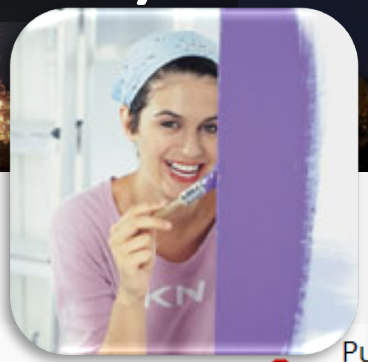
Used VAM - Vinyl Acetate Monomer plant for sale & relocation! If any interest, please contact me!

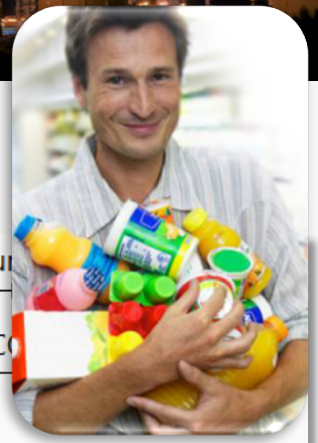
Tommy Heino
Industrialist & Entrepreneur, Owner, XHL Business Engineering
Top Contributor

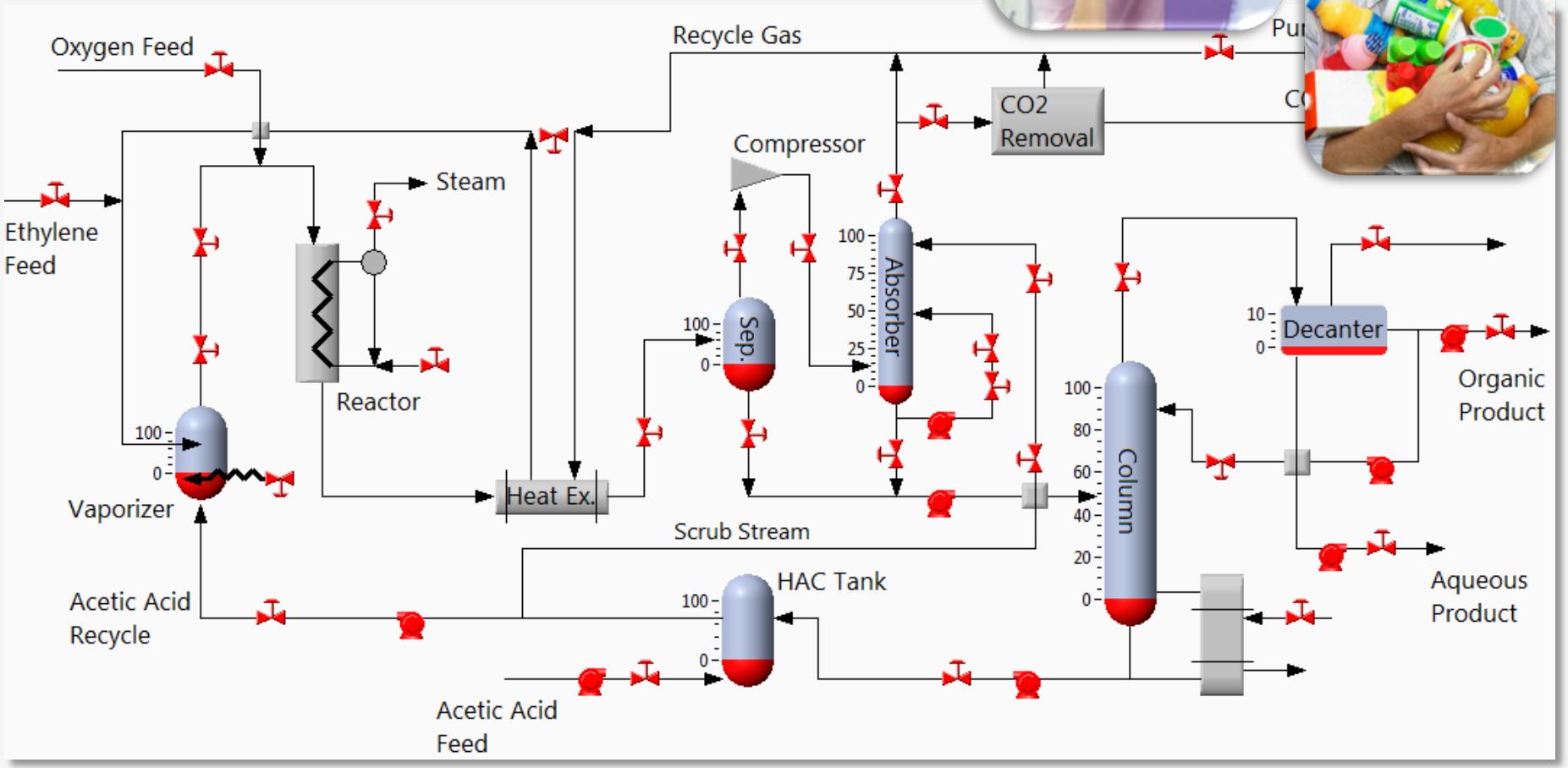
Like • Comment (4) • Share • Follow • 3 mor

More plants offers:
http://www.usedplants.com/

Vinyl Acetate Monomer plant (model)

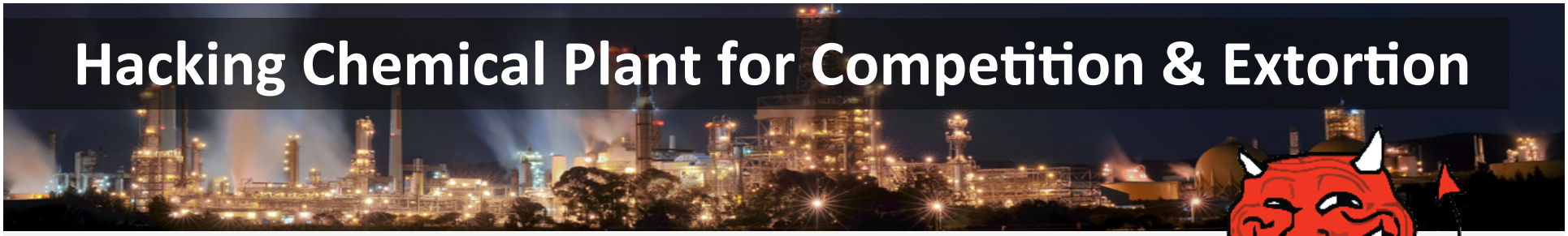




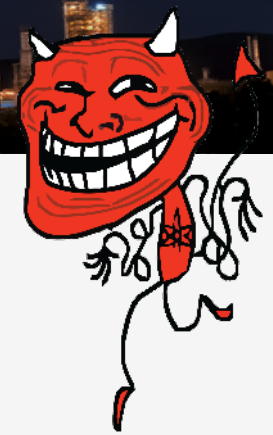


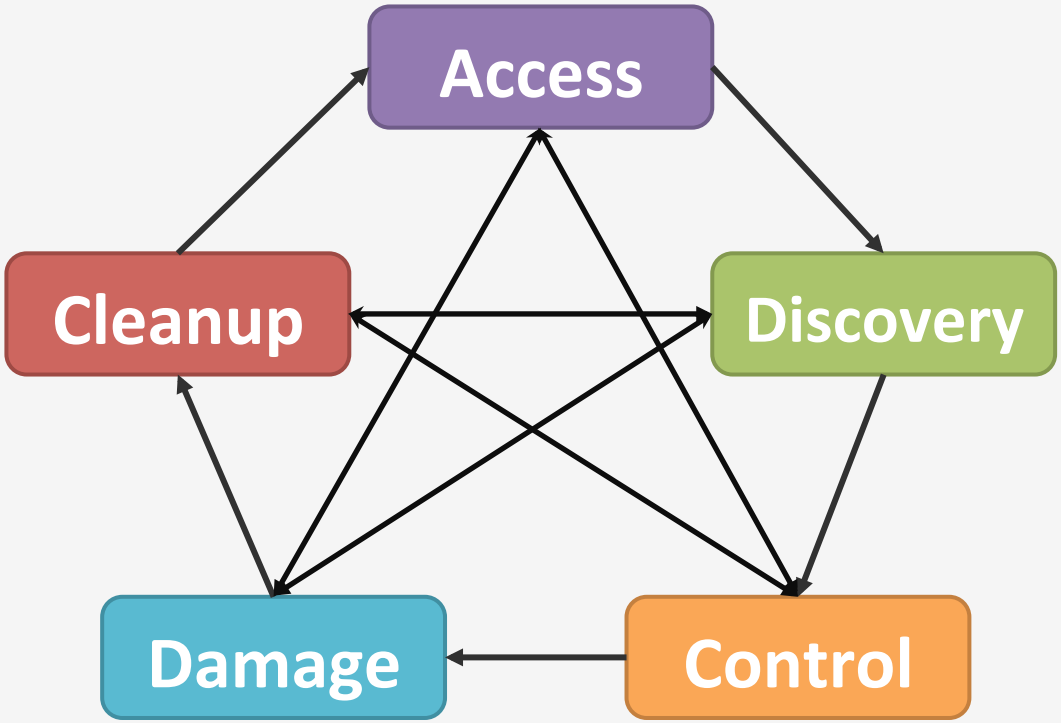
Stages of cyber-physical attacks

Hacking Chemical Plant for Competition & Extortion

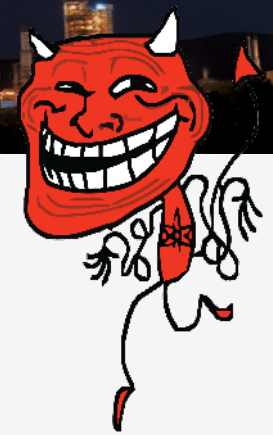


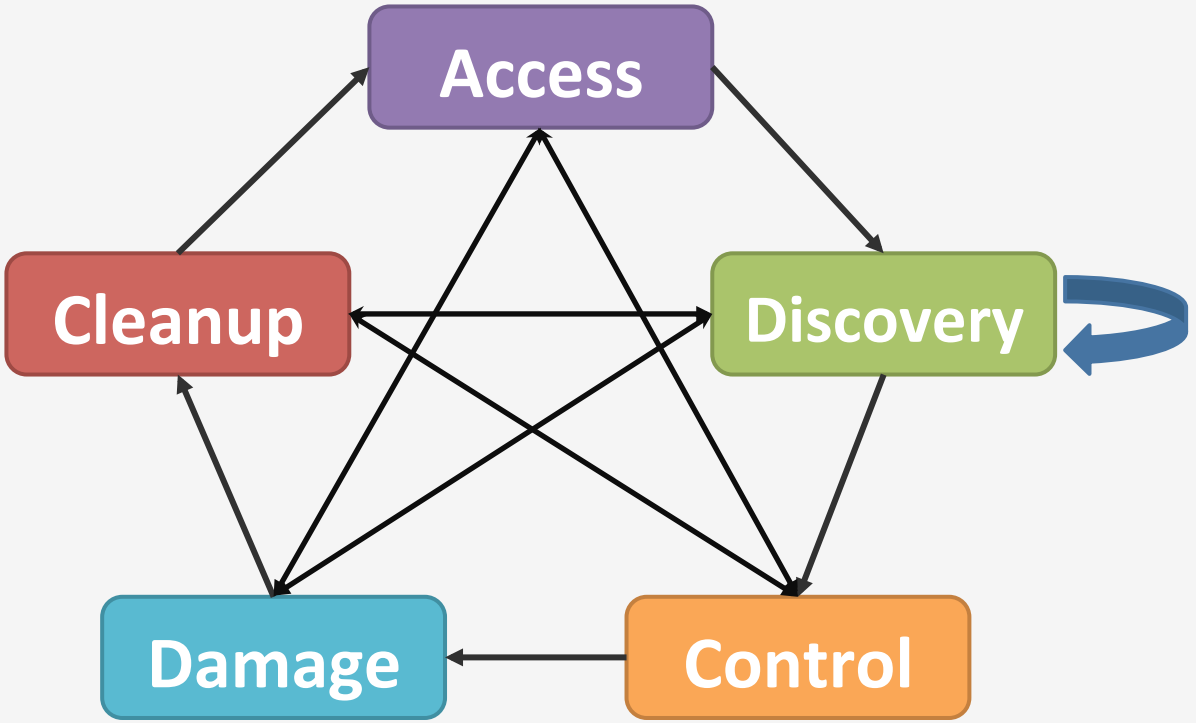
Stages of SCADA attack





Stages of SCADA attack



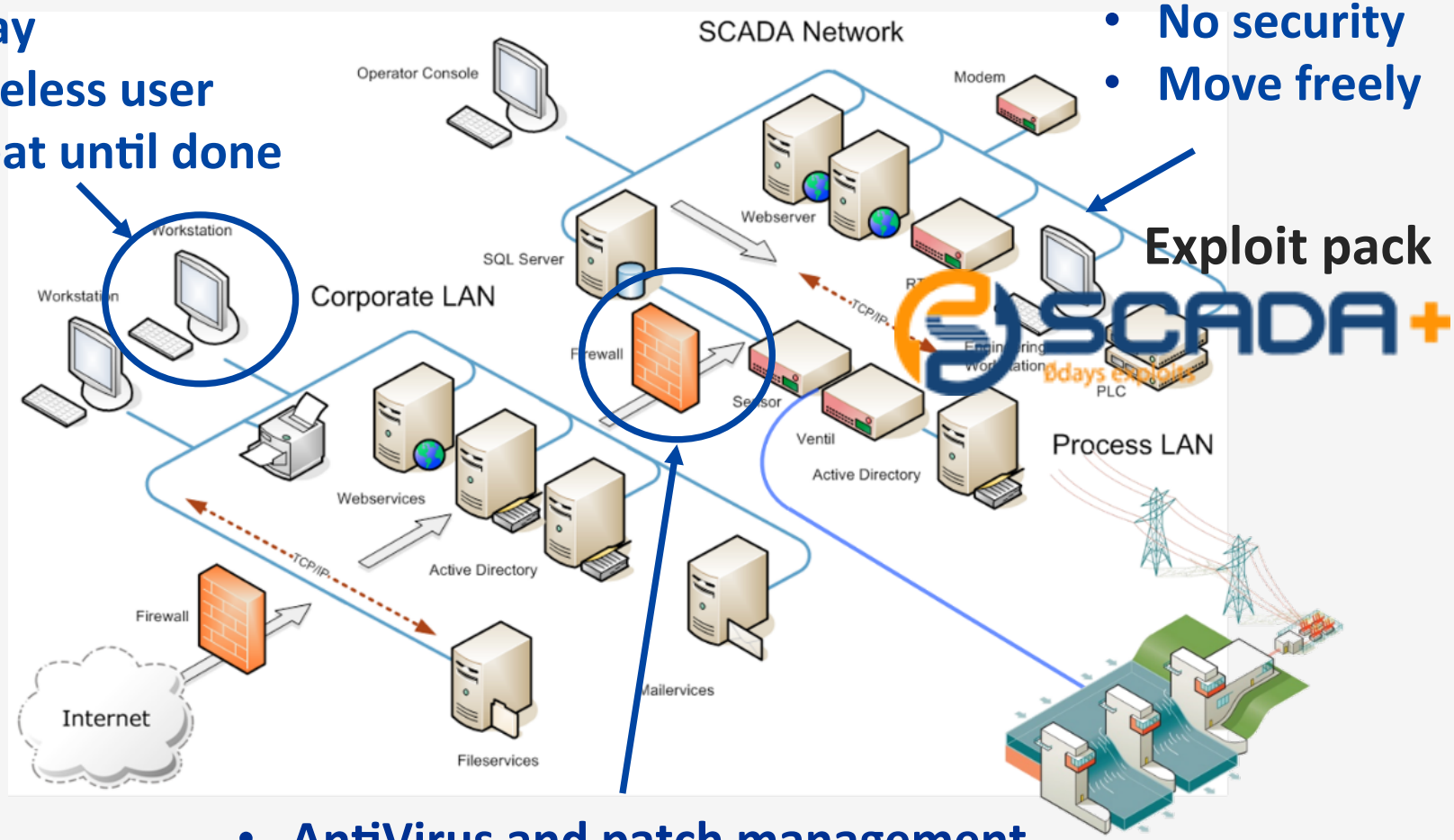


Access

Traditional IT hacking

- 1 0day
- 1 Clueless user
- Repeat until done

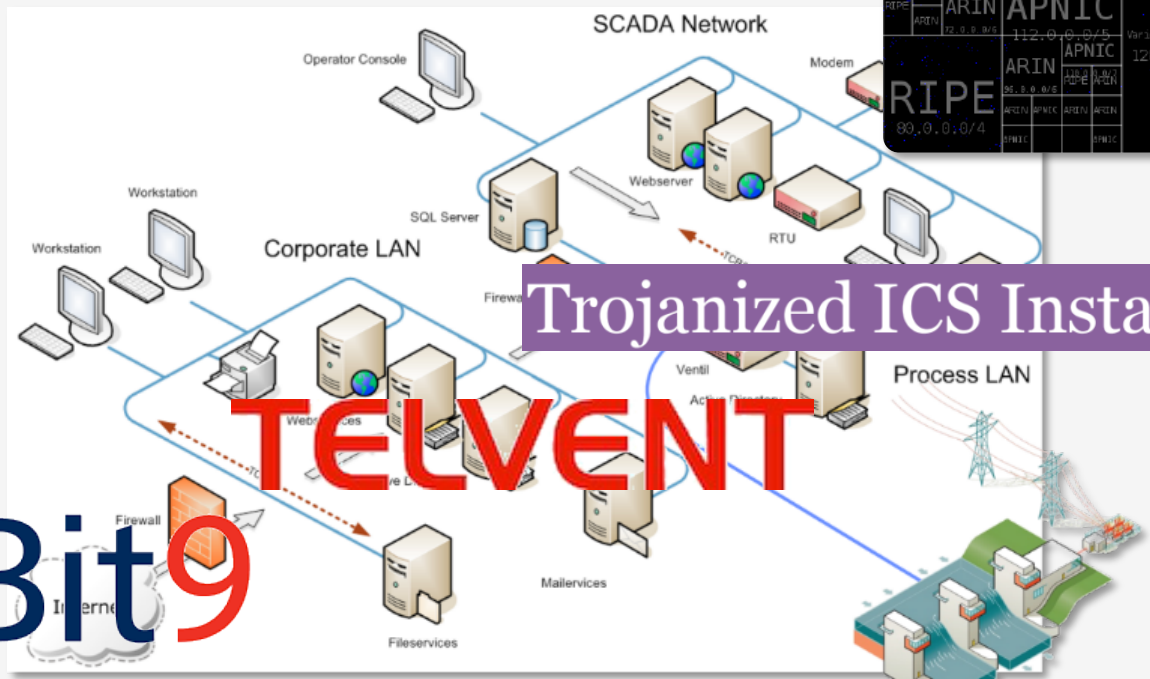
- No security
- Move freely



- AntiVirus and patch management
- Database links
- Backup systems

Modern IT hacking

- Select a vulnerability from the list of ICS-CERT advisories
- Scan Internet to locate vulnerable devices
- Exploit



- E. Leverett, R. Wightman. Vulnerability Inheritance in Programmable Logic Controllers (GreHack‘13)

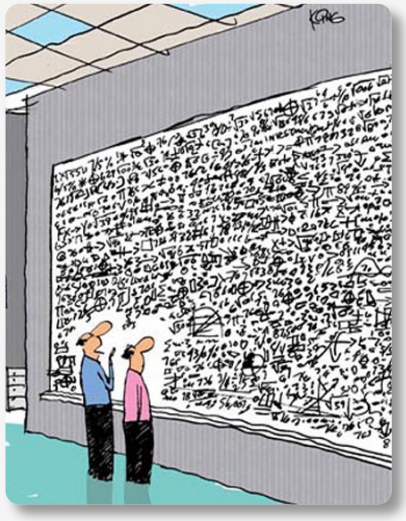
Discovery

Know the equipment

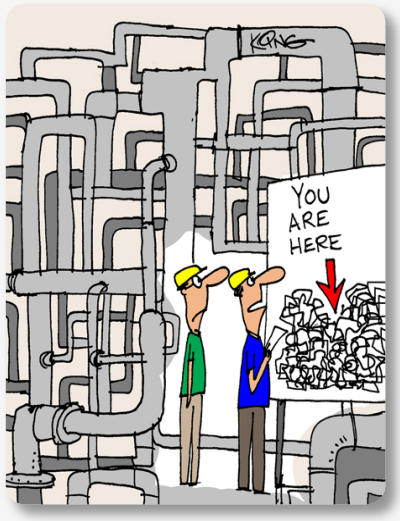
Stripping column aka stripper

Process discovery

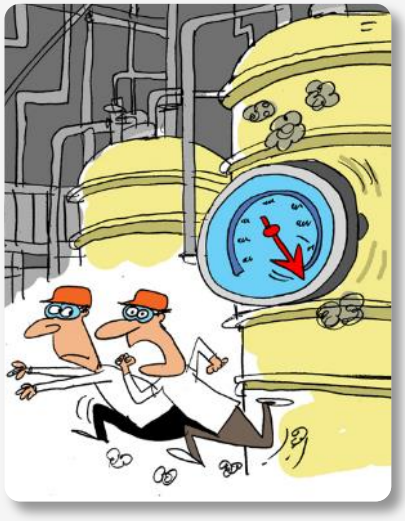
What and how the process is producing



How it is controlled



How it is build and wired



Operating and safety constraints

Espionage, reconnaissance

Target plant and third parties

Espionage

- Industrial espionage has started LONG time ago (malware samples dated as early as 2003)

Cyber Espionage comes to SCADA Security

Over Half of ICS Security Incidents Reported in 2014 Involved APTs: ICS-CERT

Nitro Malware Targeted Chemical Companies

ment, and manufacture of chemicals and advanced materials. The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes

Dragonfly: Western Energy Sector Cyberespionage campaign stole in

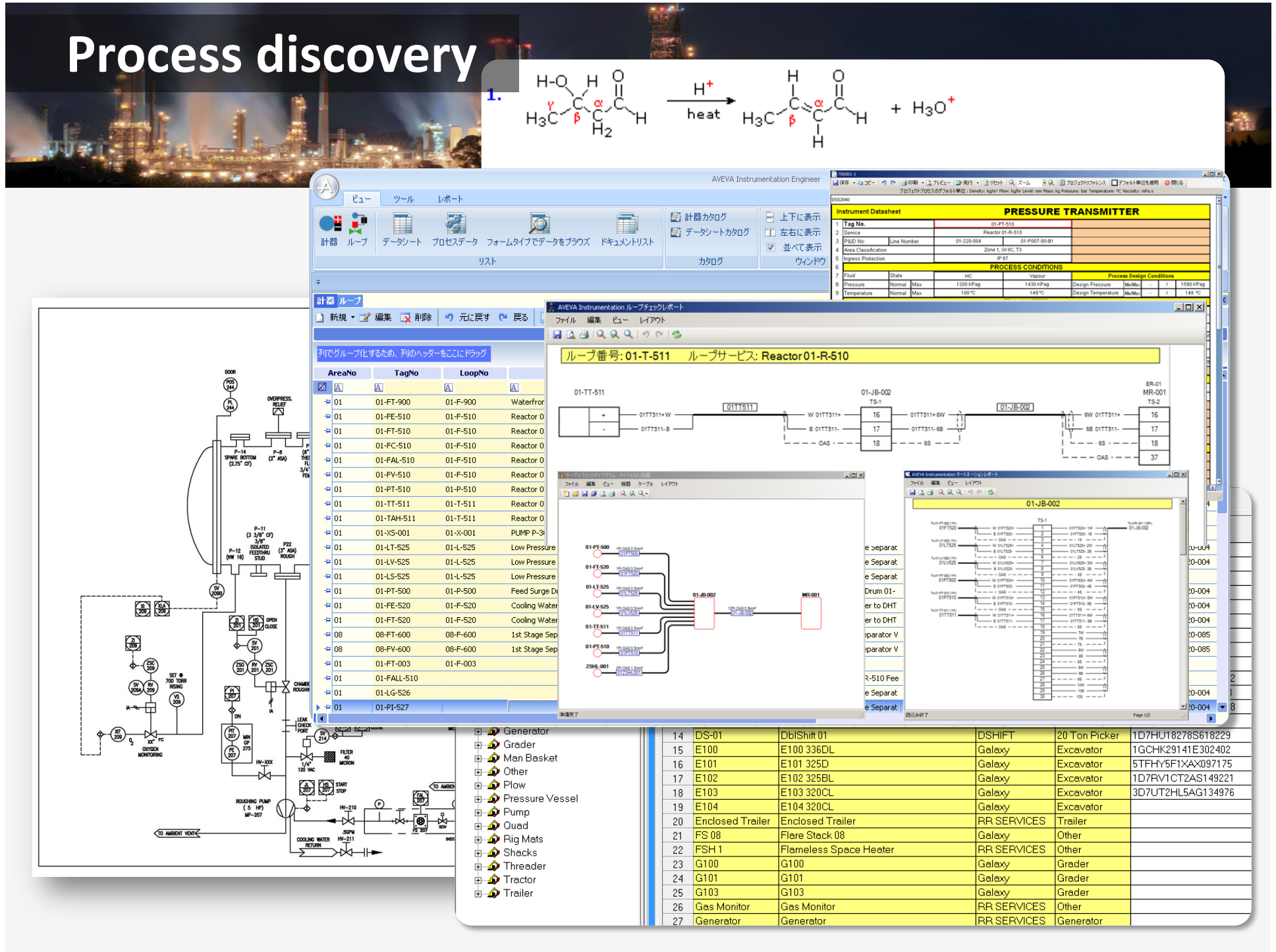
DragonFly/Havex/Ene Against Energy Suppli

ACAD/Medre.A 10000's of AutoCAD files leaked in suspected industrial espionage

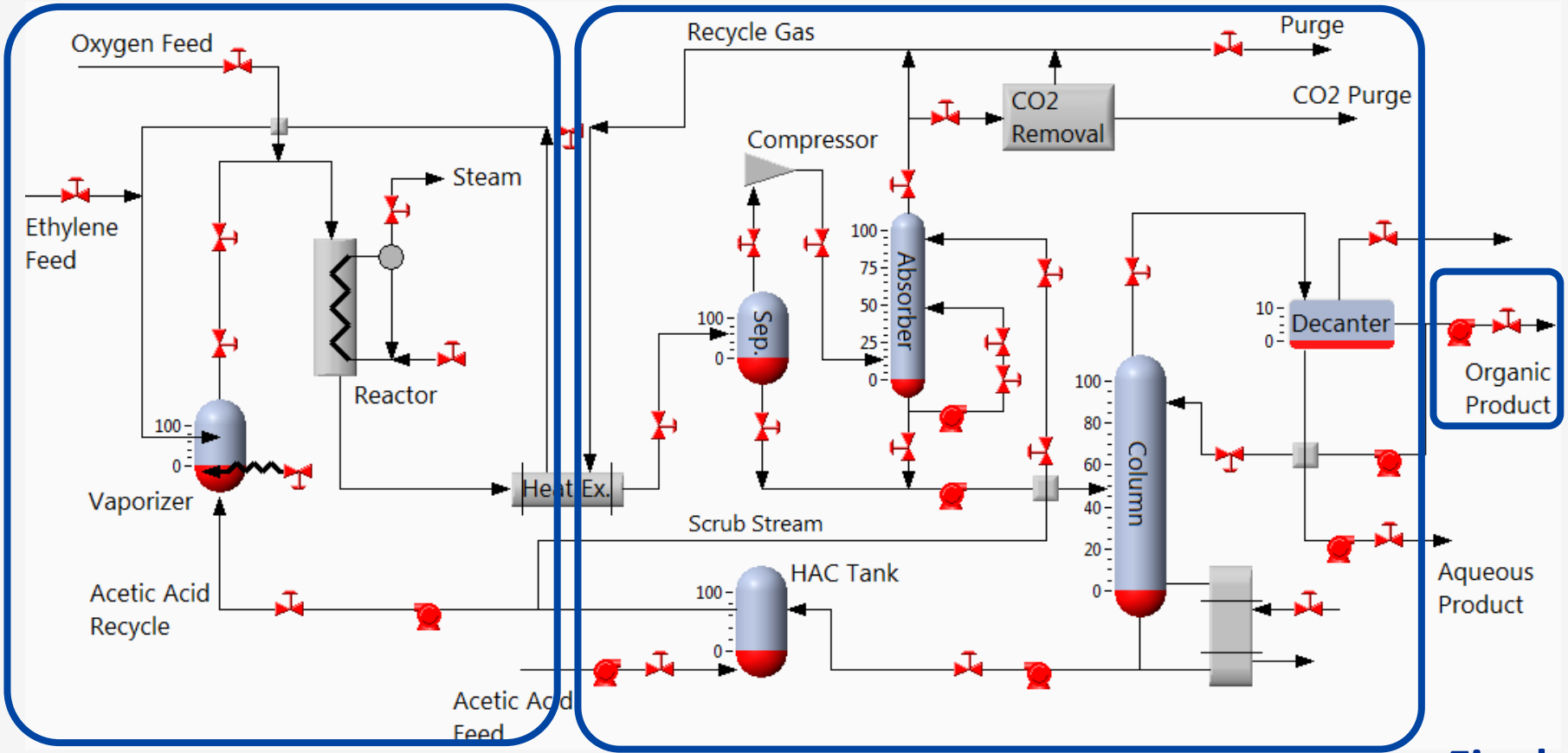
June 25, 2014

Nation state behind malware attacks on European ICS systems?

Process discovery

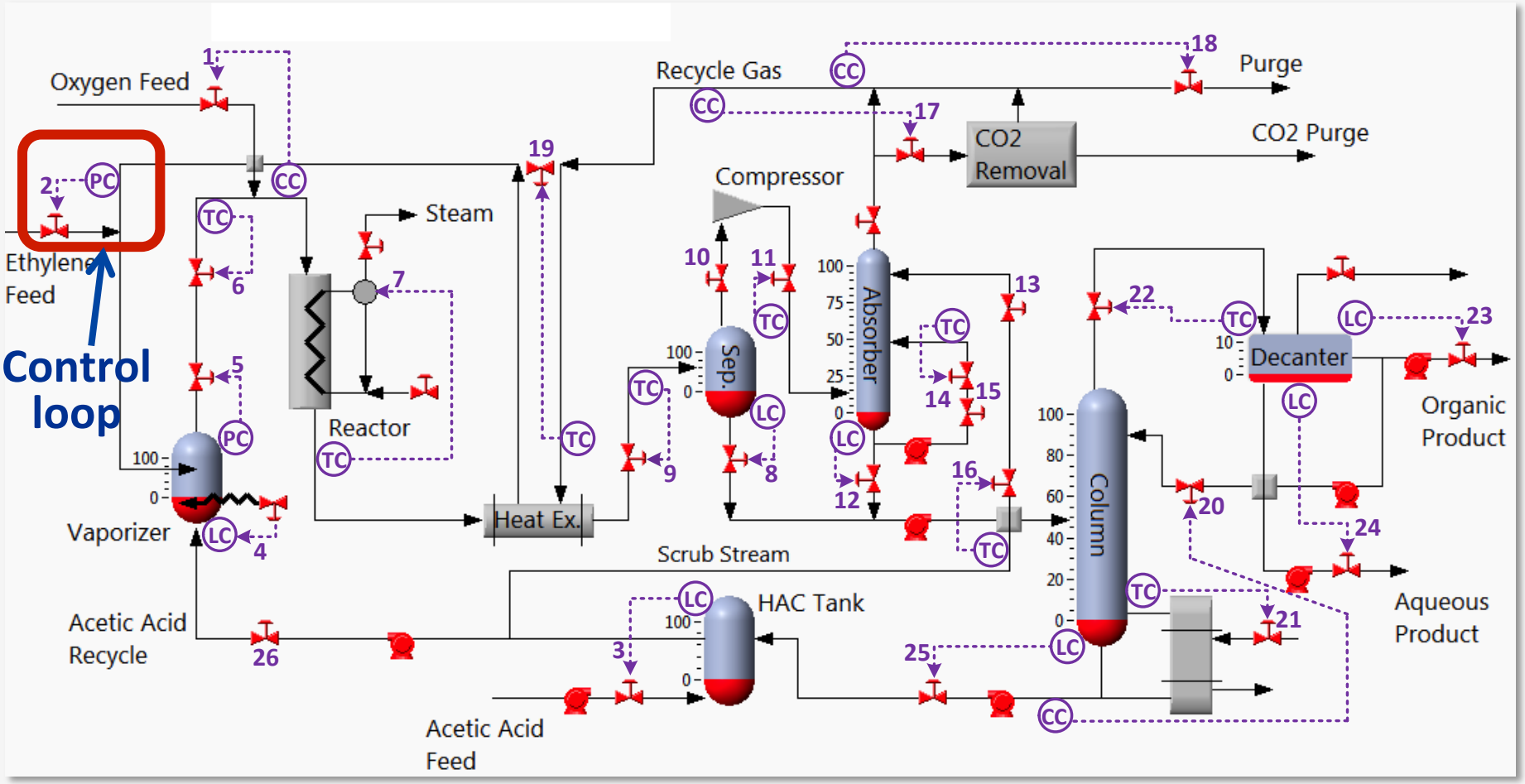


Max economic damage?

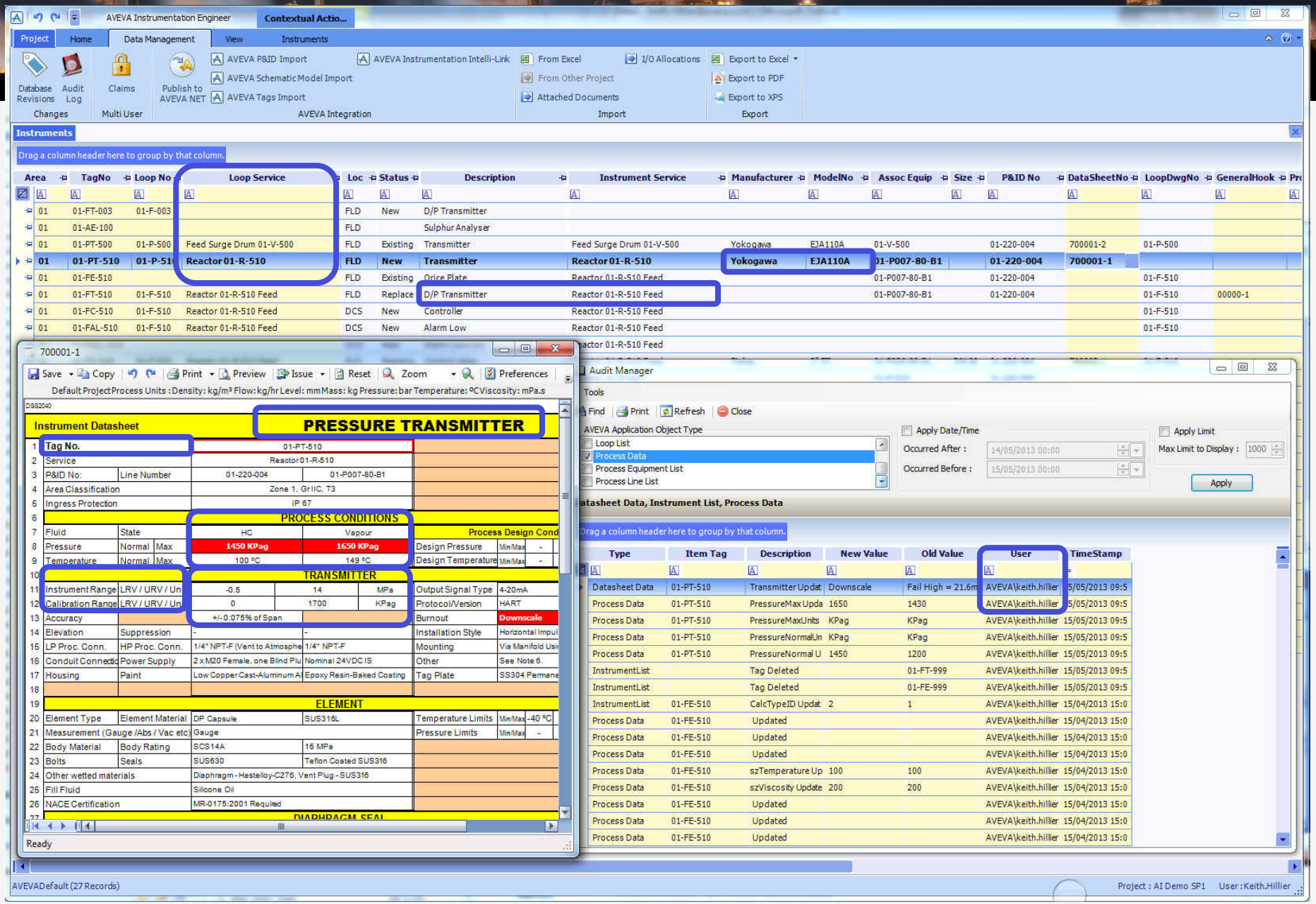


Requires input of subject matter experts

Understanding control structure

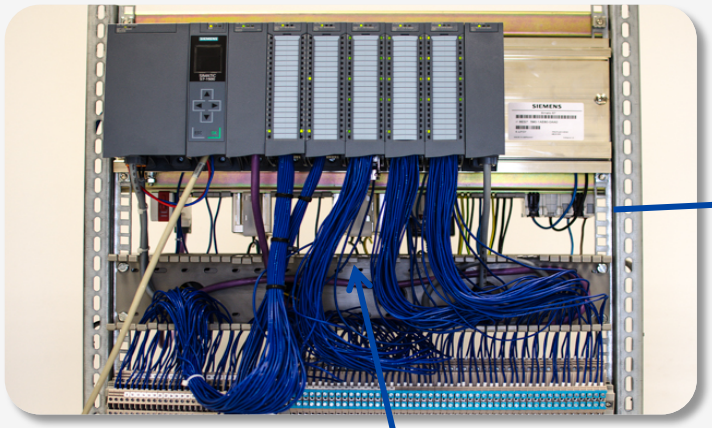


Control loop configuration

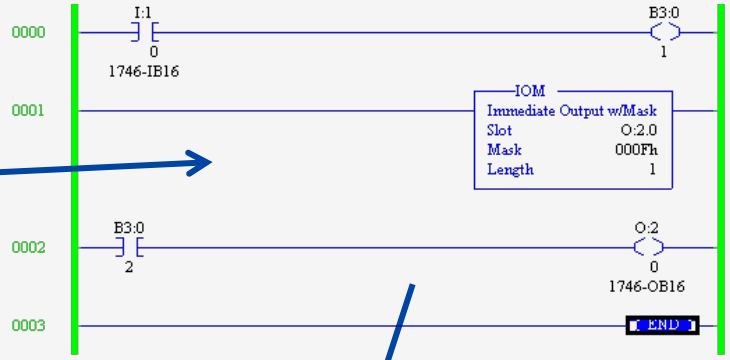


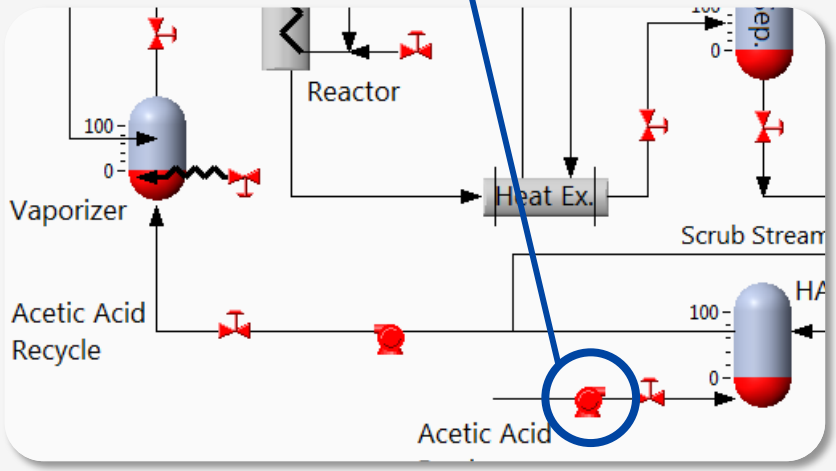
Understanding points and logic

Programmable Logic Controller

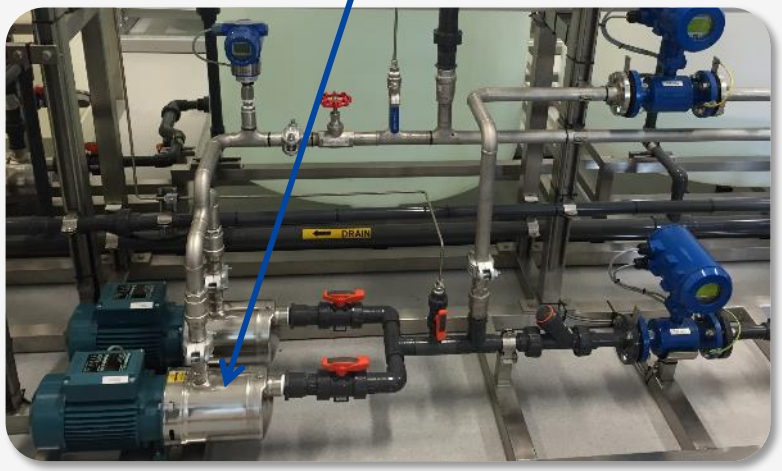


Ladder logic



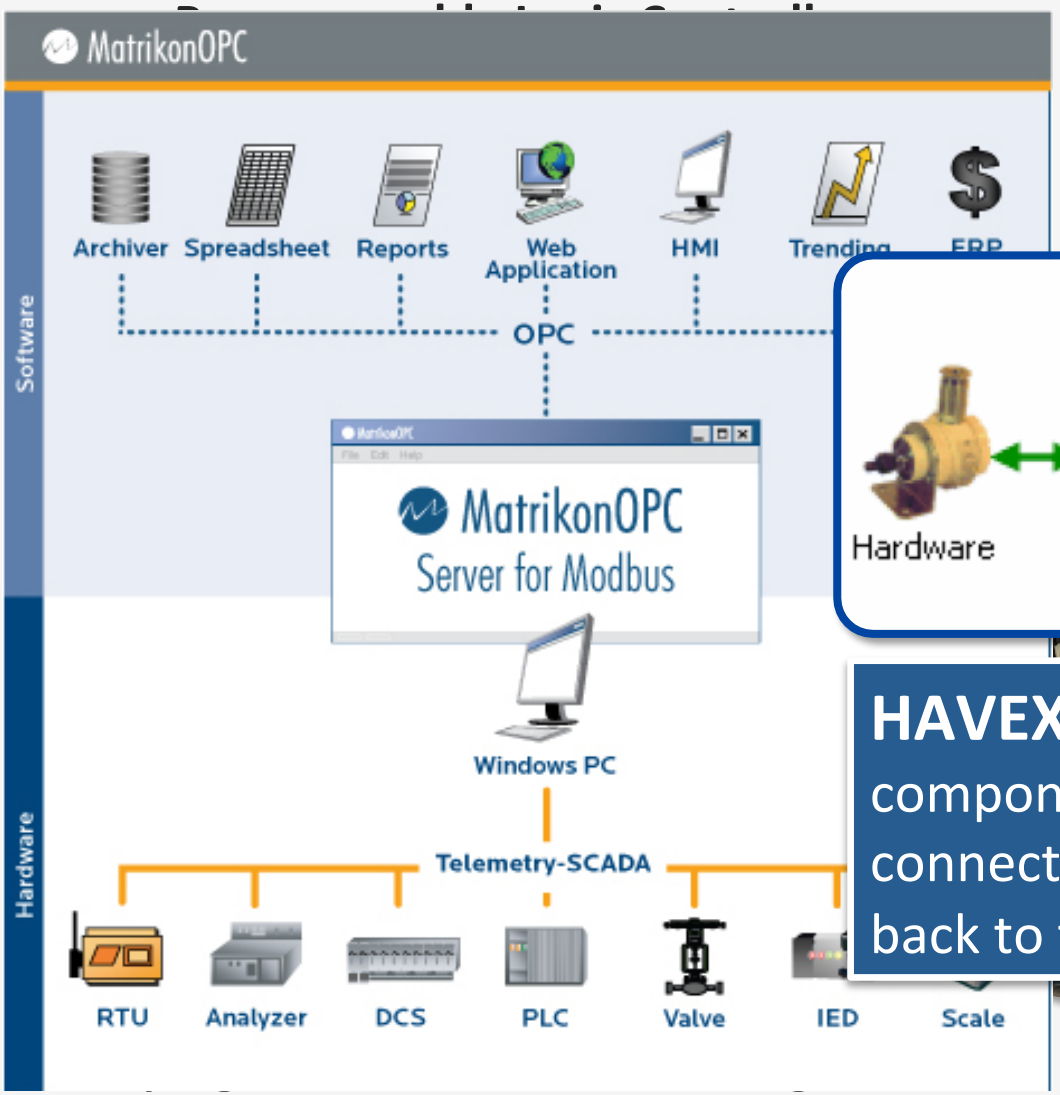


Piping and instrumentation diagram

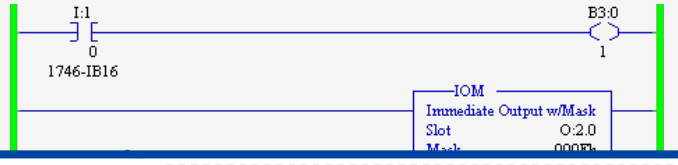


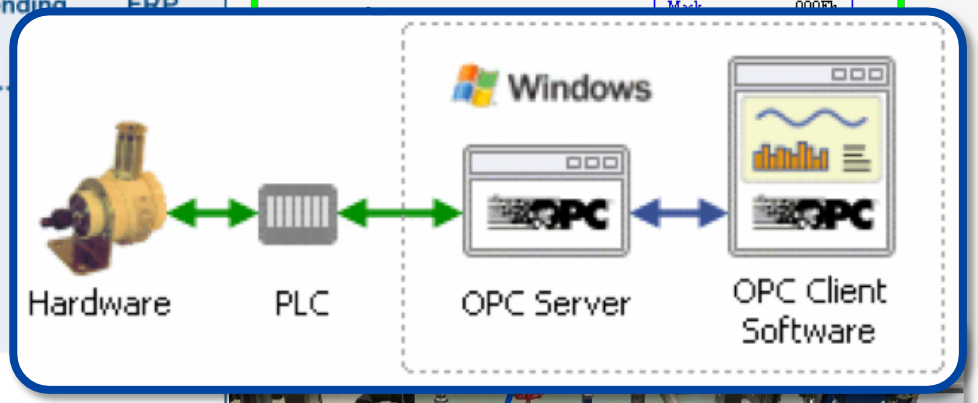
Pump in the plant

Understanding points and logic



Ladder logic

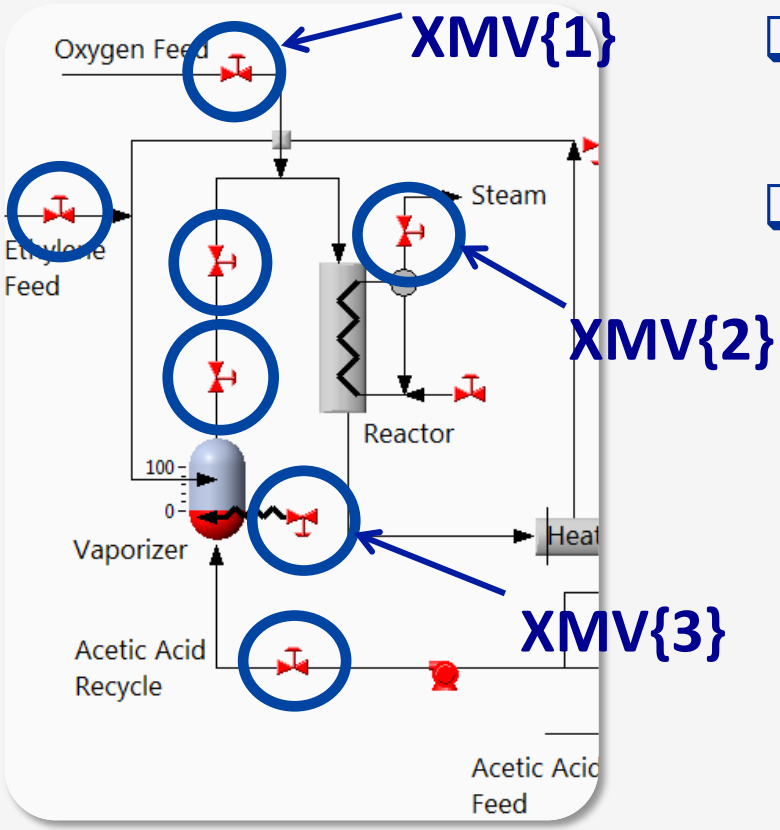




HAVEX: Using OPC, the malware component gathers any details about connected devices and sends them back to the C&C.

Pump in the plant

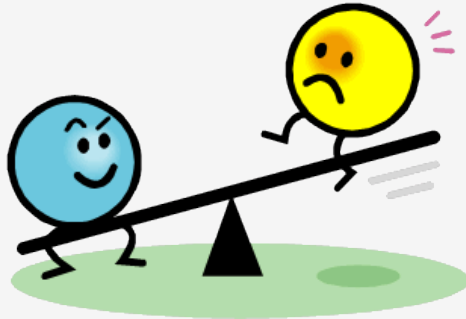
Obtaining control != being in control



- Obtained controls might not be useful for attack goal
- Attacker might not necessary be able to control obtained controls

???

Control



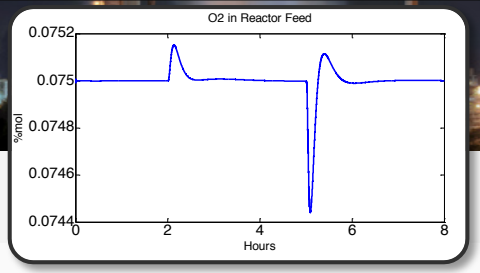
Every action has a reaction

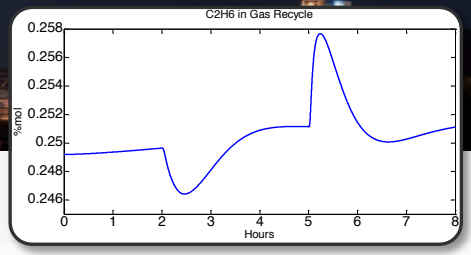
Physics of process control

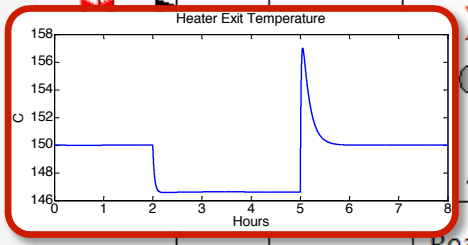
Once hooked up together, physical components become related to each other by the physics of the process

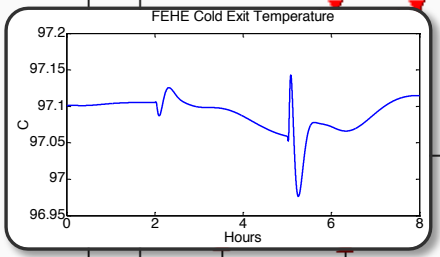
- How much does the process can be changed before releasing alarms or it shutting down?

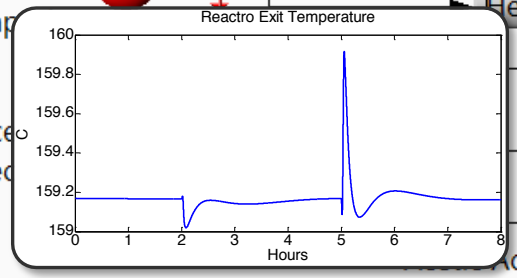
Process interdependencies

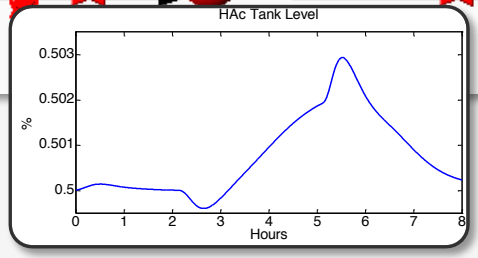


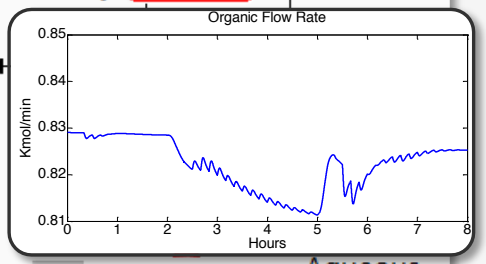




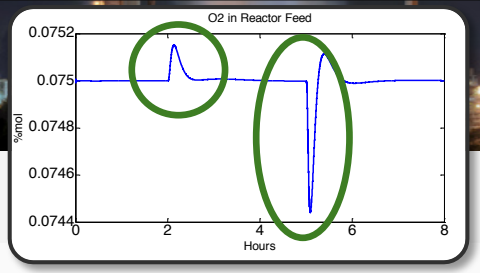


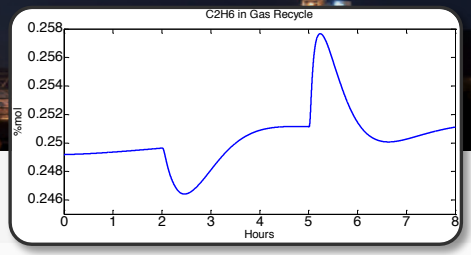


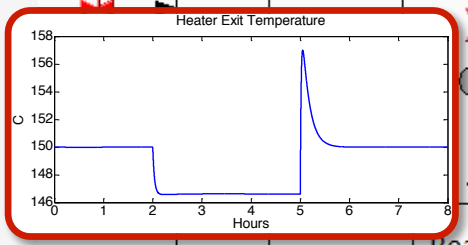


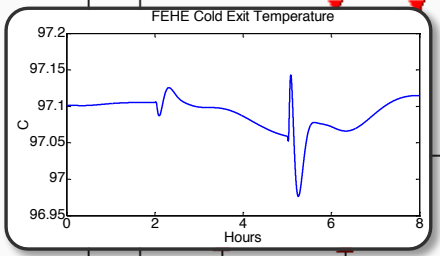


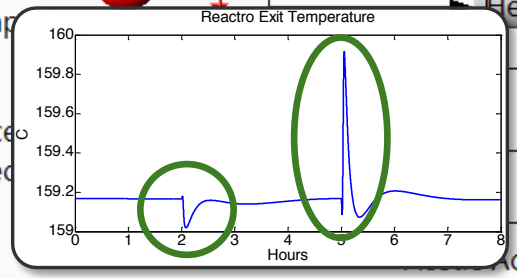
Process interdependencies

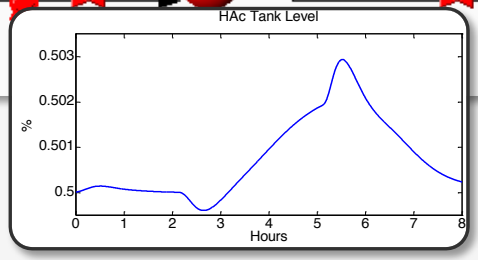


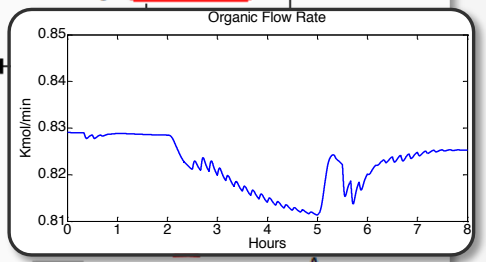












Understanding process response

- Sizing
- Dead band
- Flow properties

- Equipment design
- Process design
- Control loops coupling

- Control algorithm
- Controller tuning

- Operating practice
- Control strategy

Set point

Controller

Final control element

Process

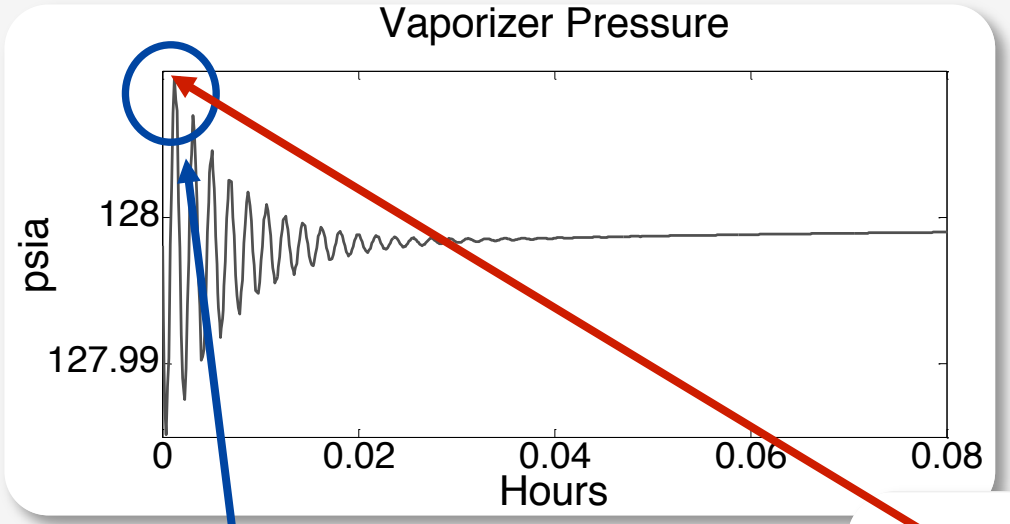
Disturbance

- Type
- Duration

Transmitter

- Sampling frequency
- Noise profile
- Filtering

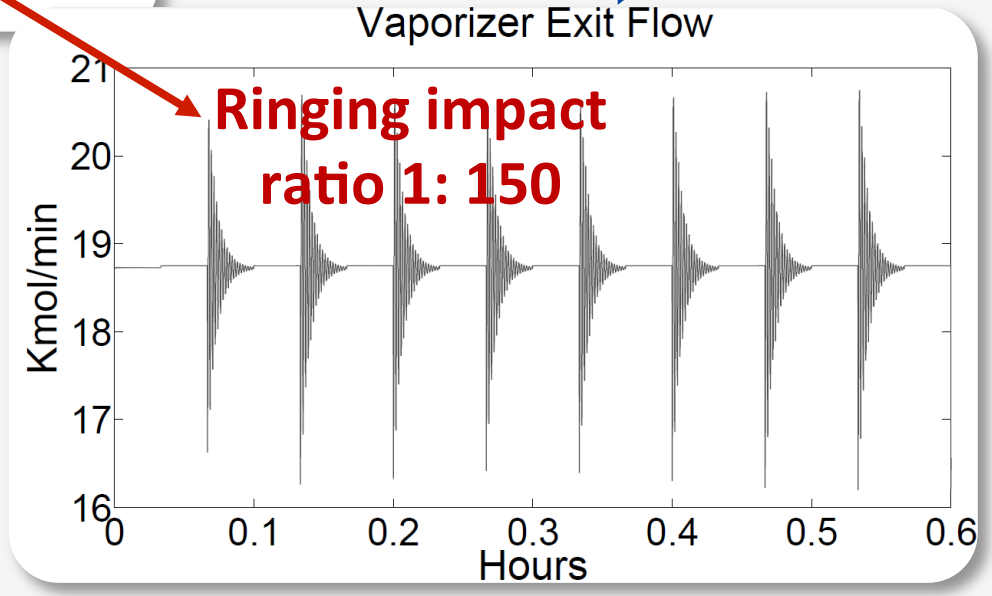
Control loop ringing



Amount of chemical entering the reactor

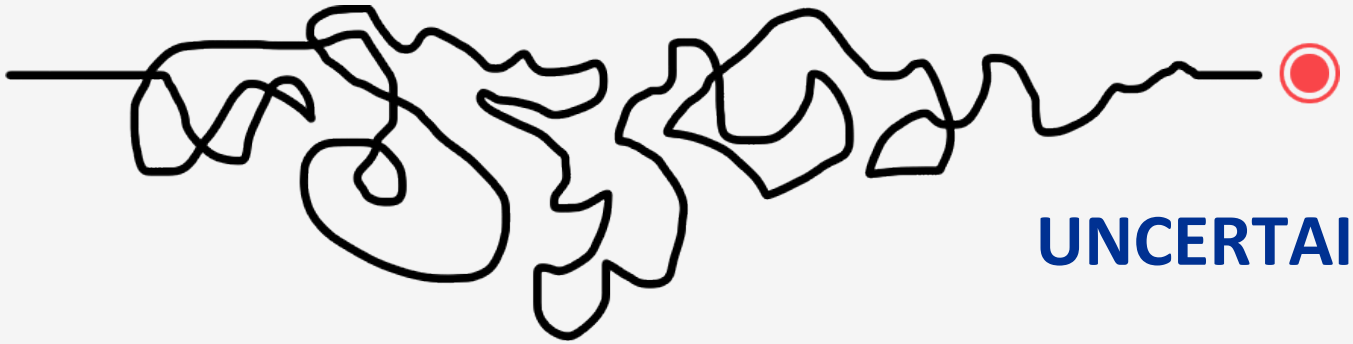
Caused by a negative real controller poles

Makes process unstable and uncontrollable



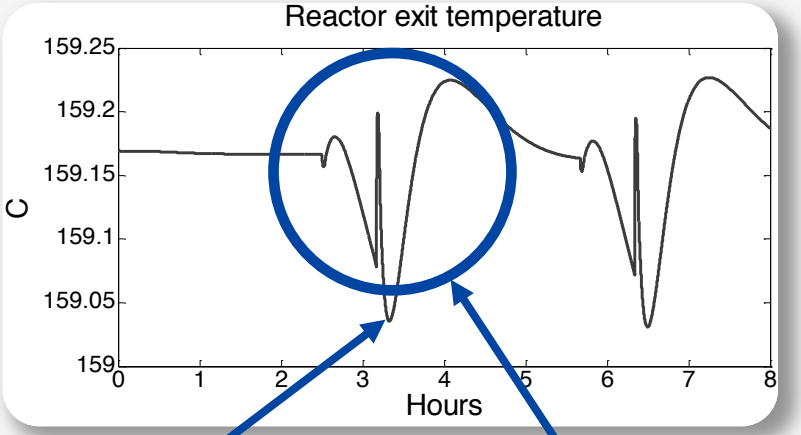
Process control challenges

- Process dynamic is highly non-linear (???)



UNCERTAINTY!

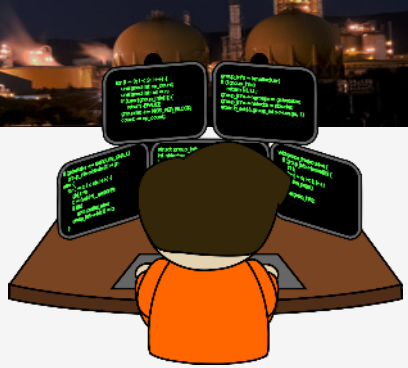
- Behavior of the process is known to the extent of its modelling
  - So to controllers. They cannot control the process beyond their control model

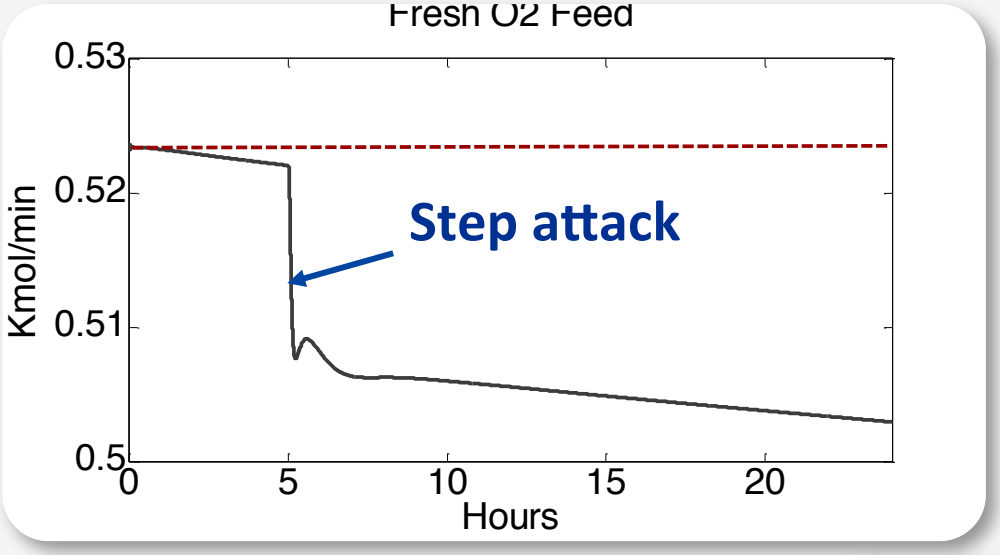


This triggers alarms

Non-liner response

Types of attacks

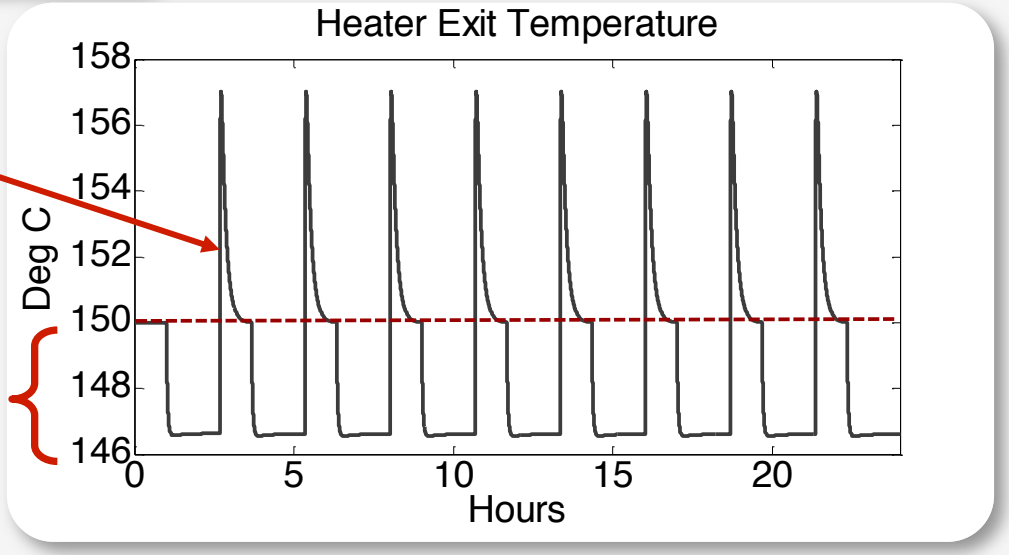




Periodic attack

Recovery time

Magnitude of manipulation



Outcome of the control stage

I am 163cm tall

We should automate this process
(work in progress)

Outcome of the control stage

Sensitivity	Magnitude of manipulation	Recovery time
High	XMV {1;5;7}	XMV {4;7}
Medium	XMV {2;4;6}	XMV {5}
Low	XMV{3}	XMV {1;2;3;6}

Reliably useful controls

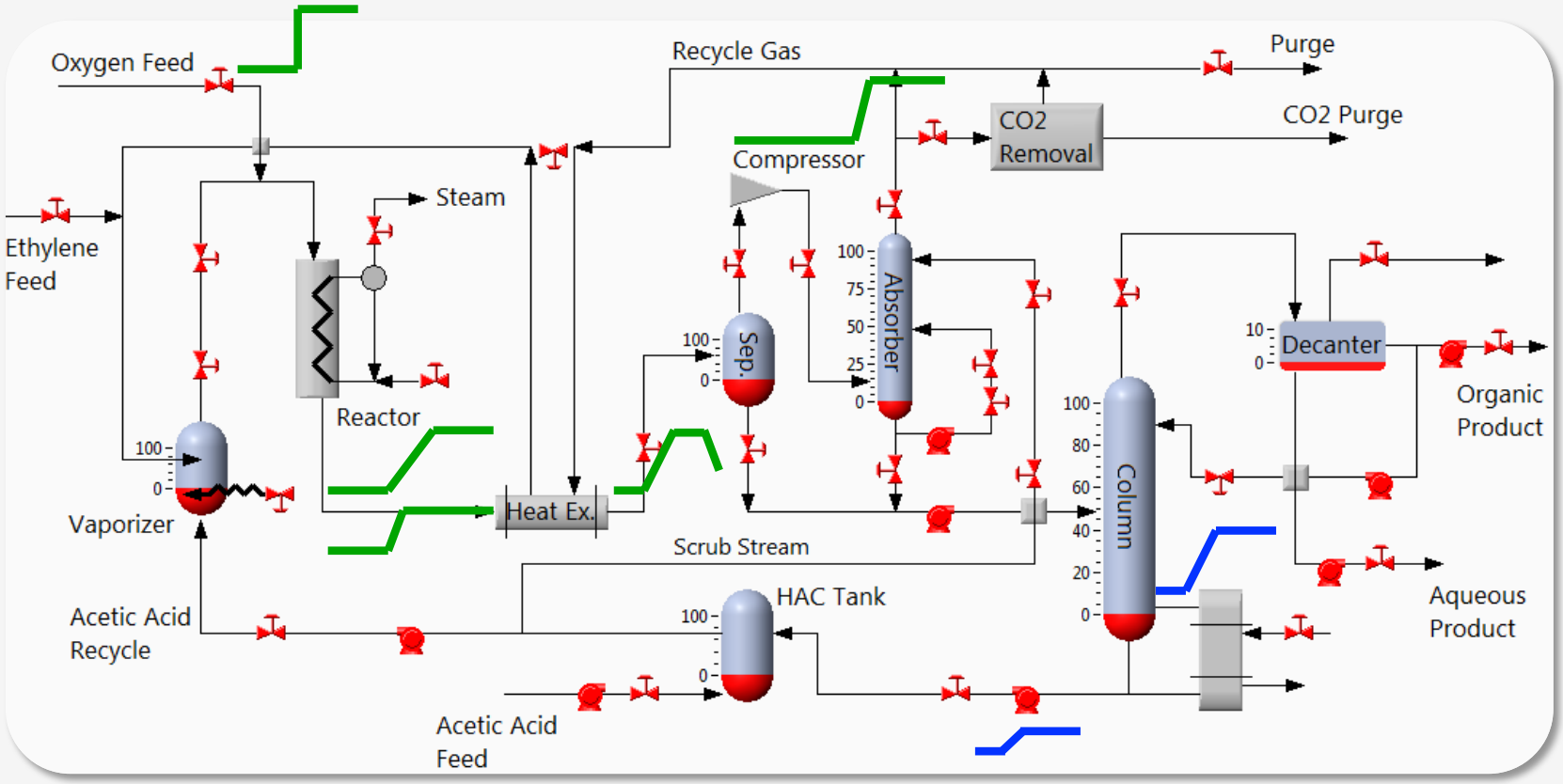
Alarm propagation

To persist we shall not bring about alarms

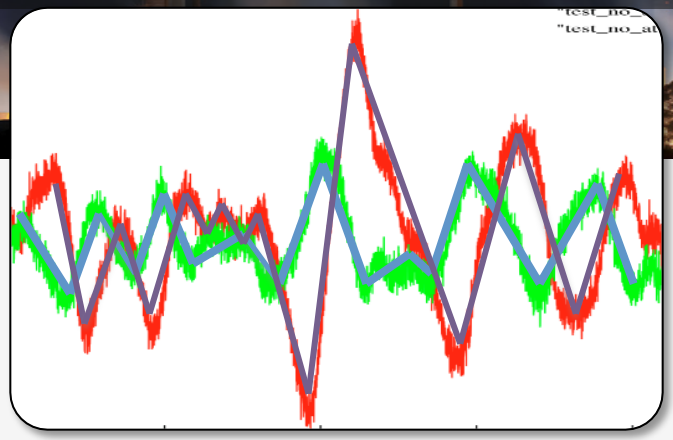
Alarm	Steady state attacks	Periodic attacks
Gas loop 02	XMV {1}	XMV {1}
Reactor feed T	XMV {6}	XMV {6}
Rector T	XMV{7}	XMV{7}
FEHE effluent	XMV{7}	XMV{7}
Gas loop P	XMV{2;3;6}	XMV{2;3;6}
HAc in decanter	XMV{2;3;7}	XMV{3}

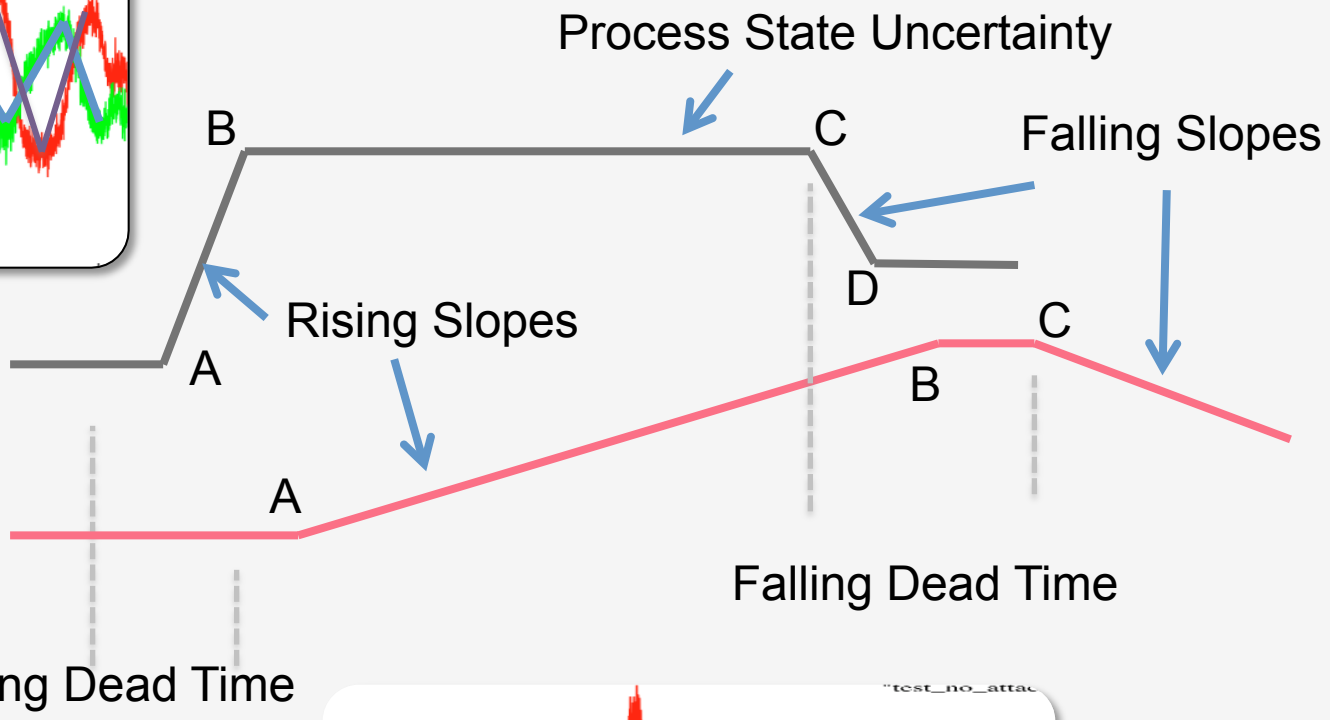
The attacker needs to figure out the marginal attack parameters which (do not) trigger alarms

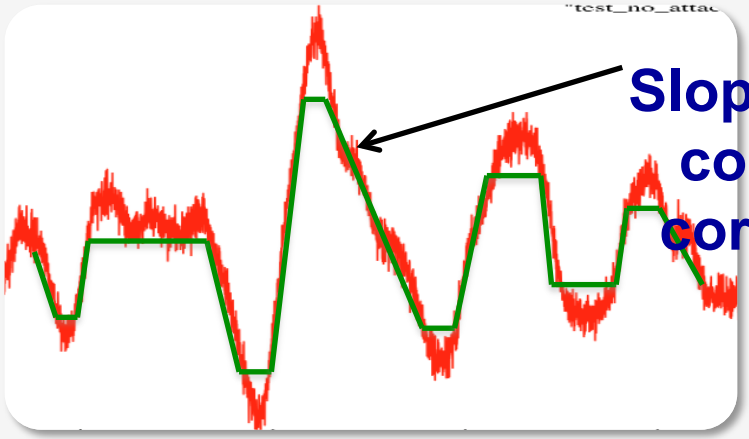
Fingerprints of plant dynamic behavior



Jason Larsen at S4x15: new triangles







Slopes: Most confident correlation

1A2A2B1B2C2D
3A2A2B2C2D2A
2B1C1D3B3C3D

Process fingerprint

Damage

How to break things?

Attacker needs one or more attack scenarios to deploy in final payload

- The least familiar stage to IT hackers
  - In most cases requires input of subject matter experts
- Accident data is a good starting point
  - Governmental agencies
  - Plants' own data bases

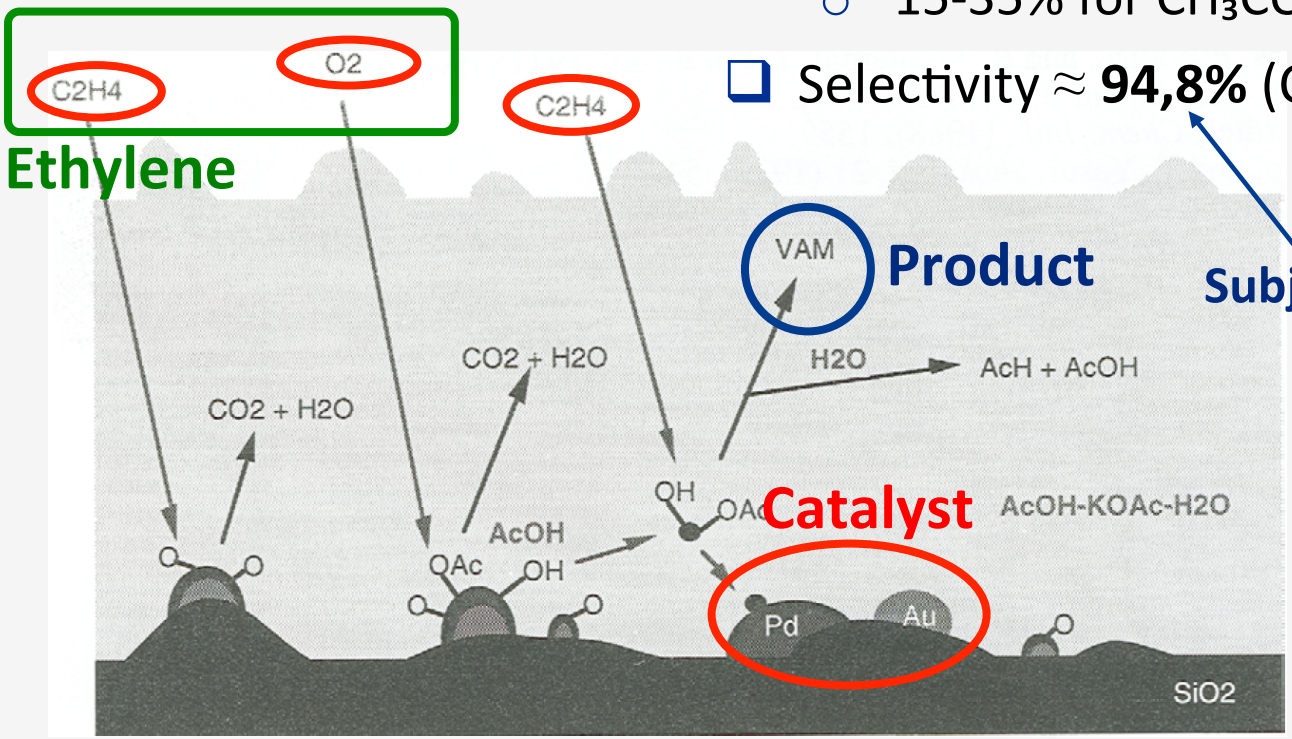
CSB OSHA

Why control before damage?

- Lifetime 1-2 years
- Low per-pass conversion
  - 15-35% for CH_3COOH and **8-10%** for C2H4
- Selectivity ≈ **94,8%** (C2H4)

On purpose low

Subjected to constant improvement



Catalyst killers

- Hot spots above 200C -> permanent deactivation
  - Lower activity at T > 180C

We were not able to rise temperature in the reactor and maintain it for long enough to cause damage to the catalyst

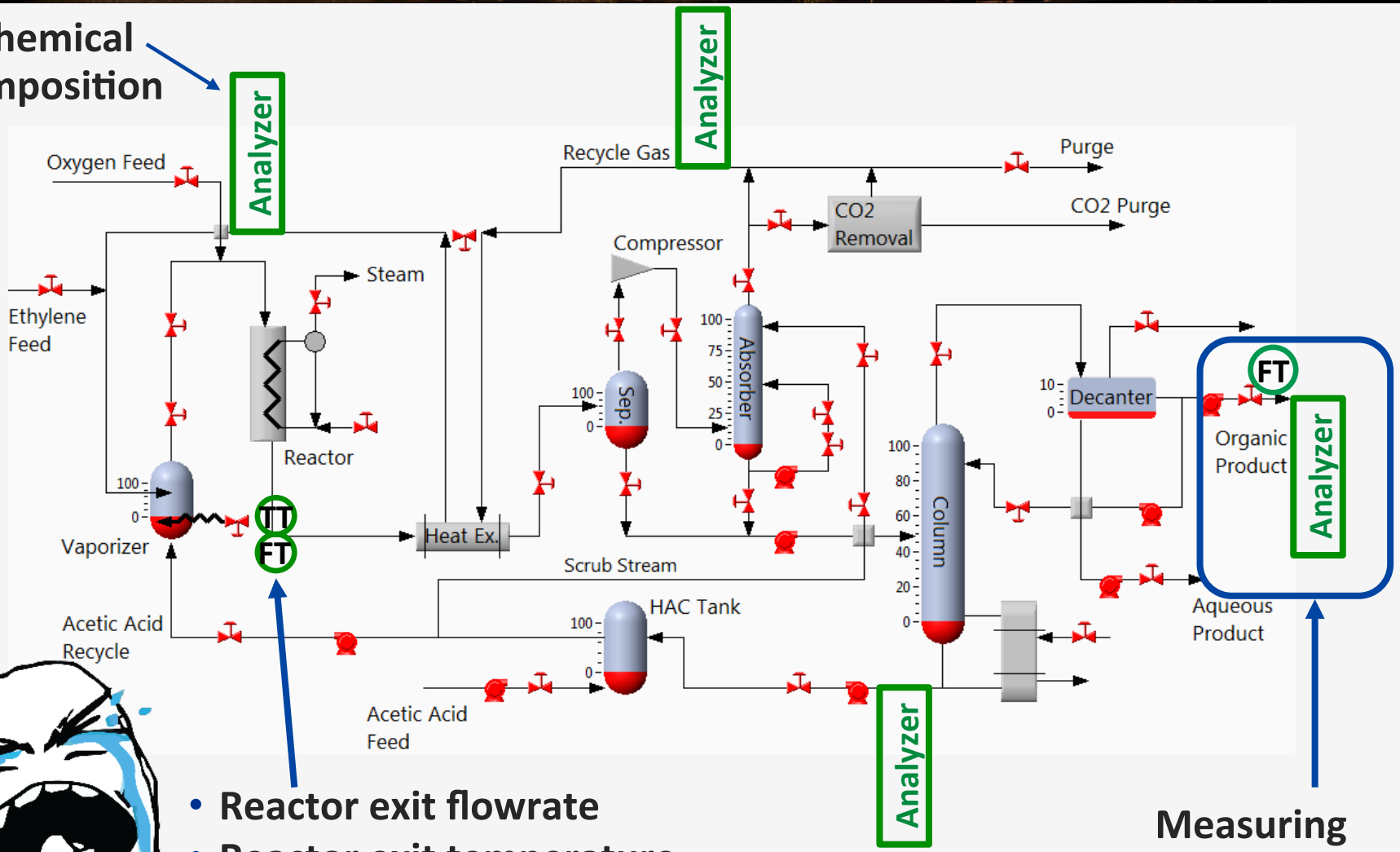
Reactor with cooling tubes

Hacker unfriendly process

- **Target plant may not have been designed in a hacker friendly way**
  - There may no sensors measuring exact values needed for the attack execution
  - The information about the process may spread across several subsystems making hacker invading more devices

Measuring the process

Chemical composition



- Reactor exit flowrate
- Reactor exit temperature
- No analyzer

Measuring here is too late

Technician vs. engineer

Technician

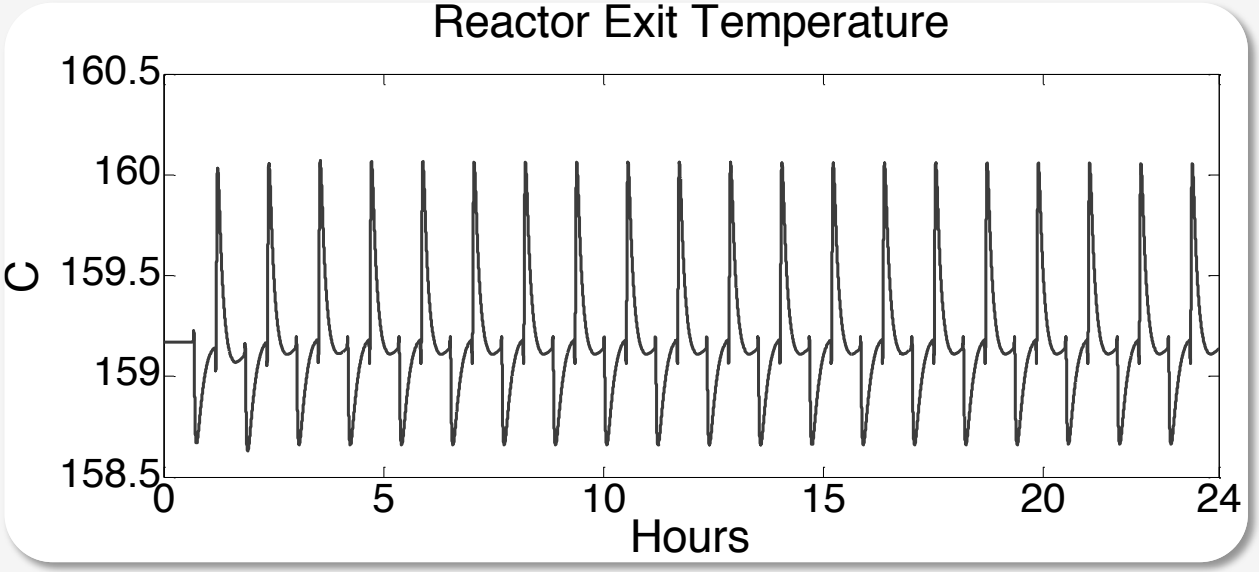
"It will eventually drain with the lowest holes loosing pressure last"

Engineer

"It will be fully drained in 20.4 seconds and the pressure curve looks like this"

Technician answer

Usage of proxy sensor



Reactor with cooling tubes

- Only tells us whether reaction rate increases or decreases
- Is not precise enough to compare effectiveness of different attacks

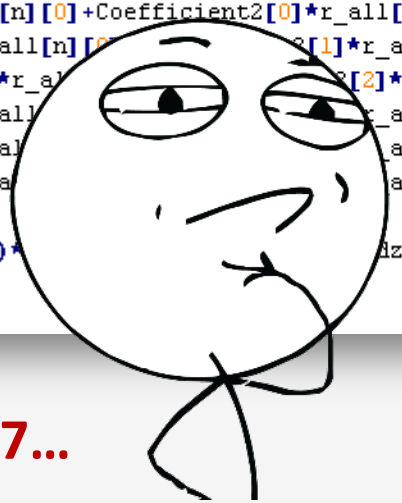
Quest for engineering answer

- Code in the controller
- Optimization applications
- Test process/plant

$$(\varepsilon\sum_{k=1}^{7} C_{i,k}Cp_{i,k} + \rho_b Cp_b)\frac{\partial T_i}{\partial t} = -\frac{\partial(v_i\sum_{k=1}^{7}(C_{i,k}Cp_{i,k})T_i)}{\partial z} - \phi_i\rho_b(r_{1,i}E_1 + r_{2,i}E_2) - Q_i^{RCT}$$

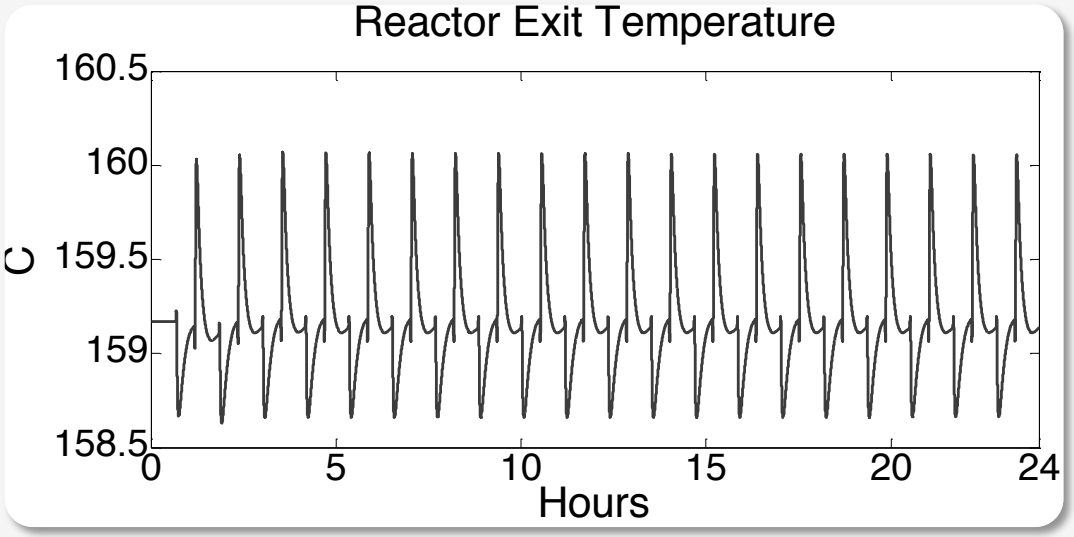
```
/*calculate derivatives*/
for (n=1;n<NR;n++)
{
    /*dC/dt=-delta(C*v)/deltaZ+sum(vij*rj)
    /*Use single backward                                    */
    C_O2_t[n-1]=(-(C_O2[n]*v[n]-C_O2[n-1]*v[n-1])/dz + Coefficient1[0]*r_all[n][0]+Coefficient2[0]*r_all[n][1])/cata_porosity;
    C_CO2_t[n-1]=(-(C_CO2[n]*v[n]-C_CO2[n-1]*v[n-1])/dz + Coefficient1[1]*r_all[n][ [1]*r_all[n][1])/cata_porosity;
    C_C2H4_t[n-1]=(-(C_C2H4[n]*v[n]-C_C2H4[n-1]*v[n-1])/dz + Coefficient1[2]*r_a [2]*r_all[n][1])/cata_porosity;
    C_VAc_t[n-1]=(-(C_VAc[n]*v[n]-C_VAc[n-1]*v[n-1])/dz + Coefficient1[4]*r_all _all[n][1])/cata_porosity;
    C_H2O_t[n-1]=(-(C_H2O[n]*v[n]-C_H2O[n-1]*v[n-1])/dz + Coefficient1[5]*r_a  all[n][1])/cata_porosity;
    C_HAc_t[n-1]=(-(C_HAc[n]*v[n]-C_HAc[n-1]*v[n-1])/dz + Coefficient1[6]*r_a  all[n][1])/cata_porosity;
    Q_rct[n]= UA*(Tg[n]-Shell_T); /*kcal/min m^3*/
    Tg_t[n-1]=1/(cata_porosity*CCP[n] + cata_heatcapacity *cata_bulk_density)*  dz - r_all[n][0]*E_r1-r_all[
    n][1]*E_r2-Q_rct[n]);
};
```

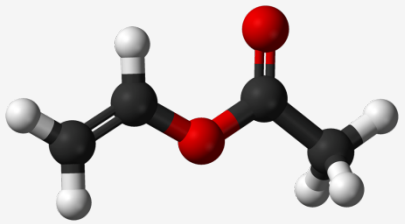
CHALLENGE CONSIDERED



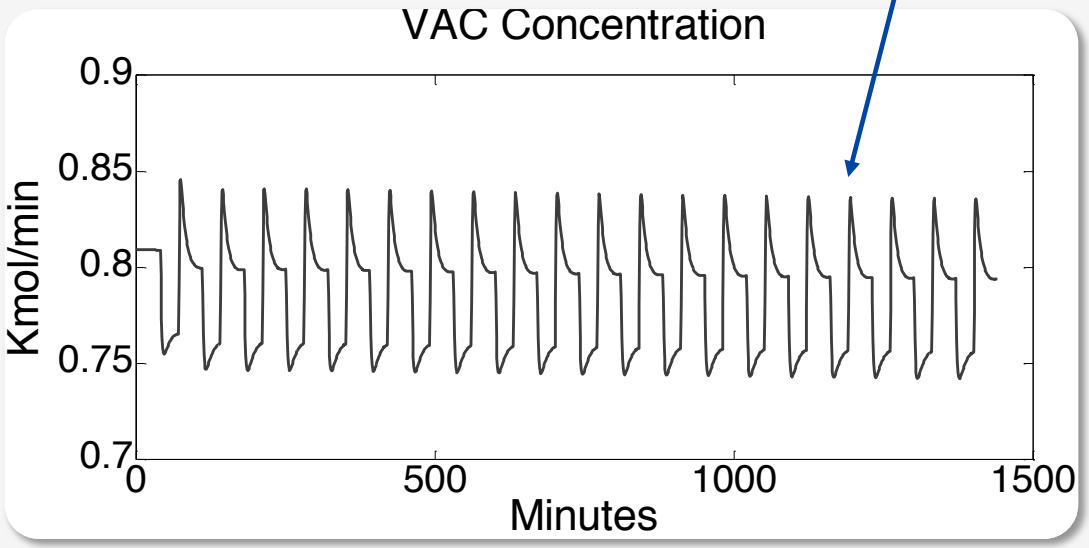
0,00073; 0,00016; 0,0007…

Engineering answer

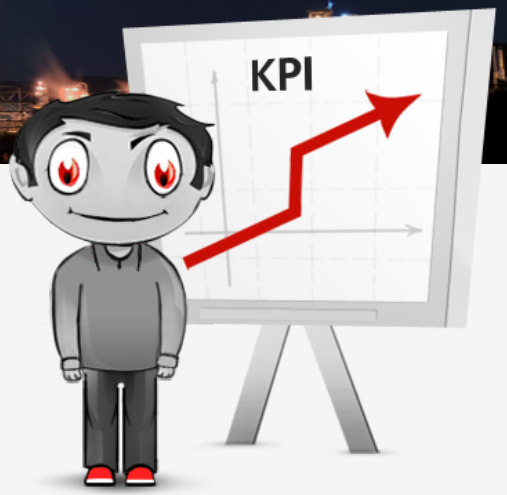




Vinyl Acetate production

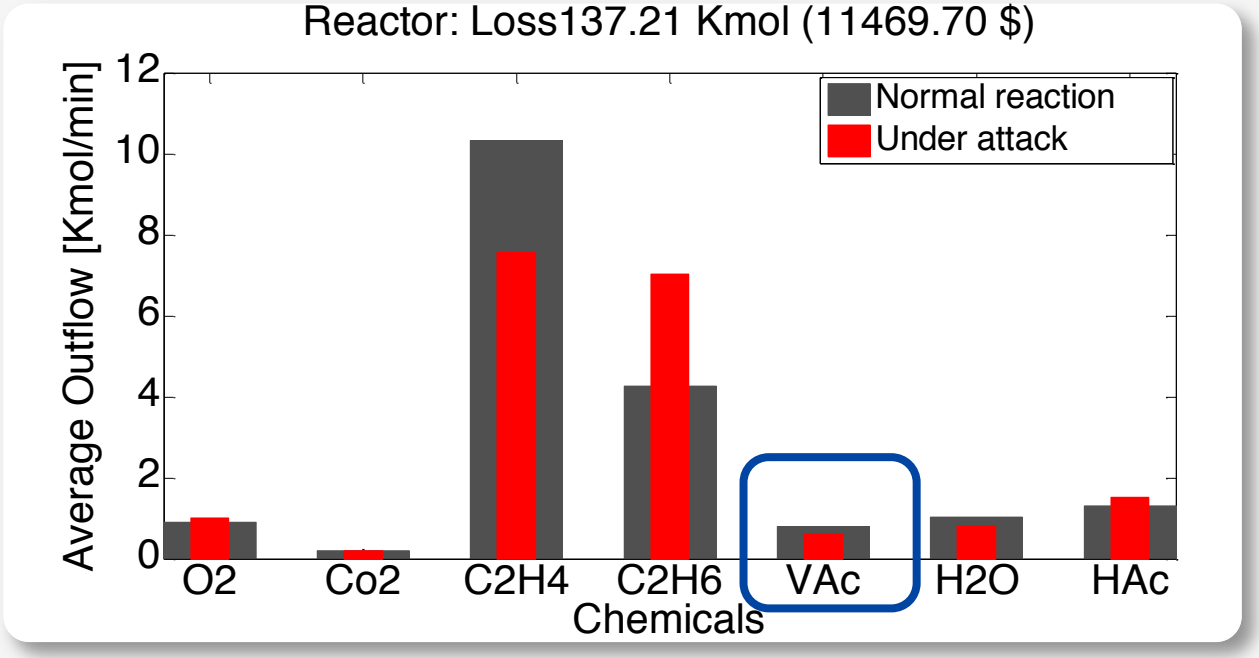


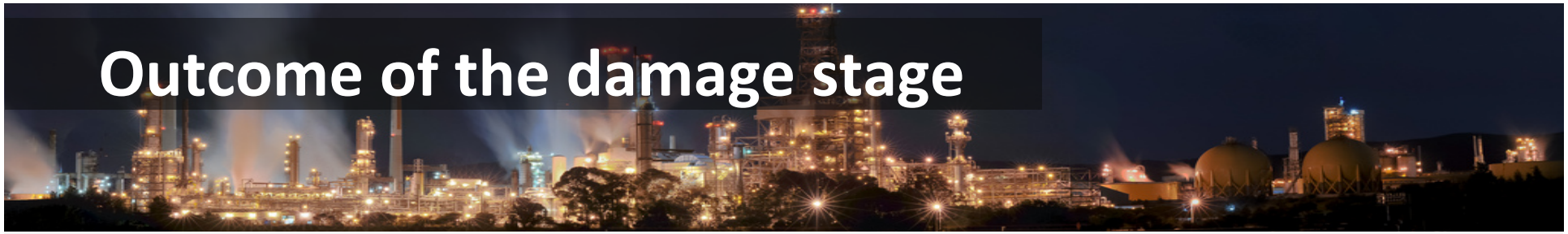
Product loss



Product per day: 96.000$

Product loss per day: 11.469,70$





Outcome of the damage stage

Product per day: 96.000$

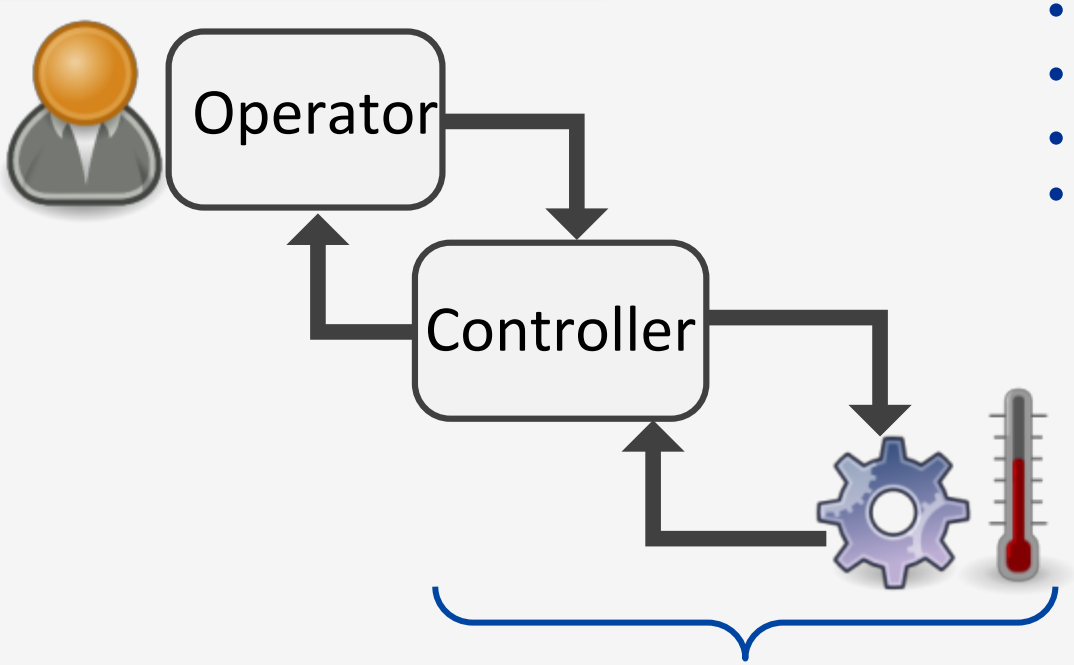
Product loss, 24 hours	Steady-state attacks	Periodic attacks
High, ≥ 10.000$	XMV {2}	XMV {4;6}
Medium, 5.000$ - 10.000$	XMV {6;7}	XMV {5;7}
Low, 2.000$ - 5.000$	-	XMV {2}
Negligible, ≤ 2.000$	XMV {1;3}	XMV {1;2}

Still might be useful

Clean-up

Socio-technical system

- Maintenance stuff
- Plant engineers
- Process engineers
- ….



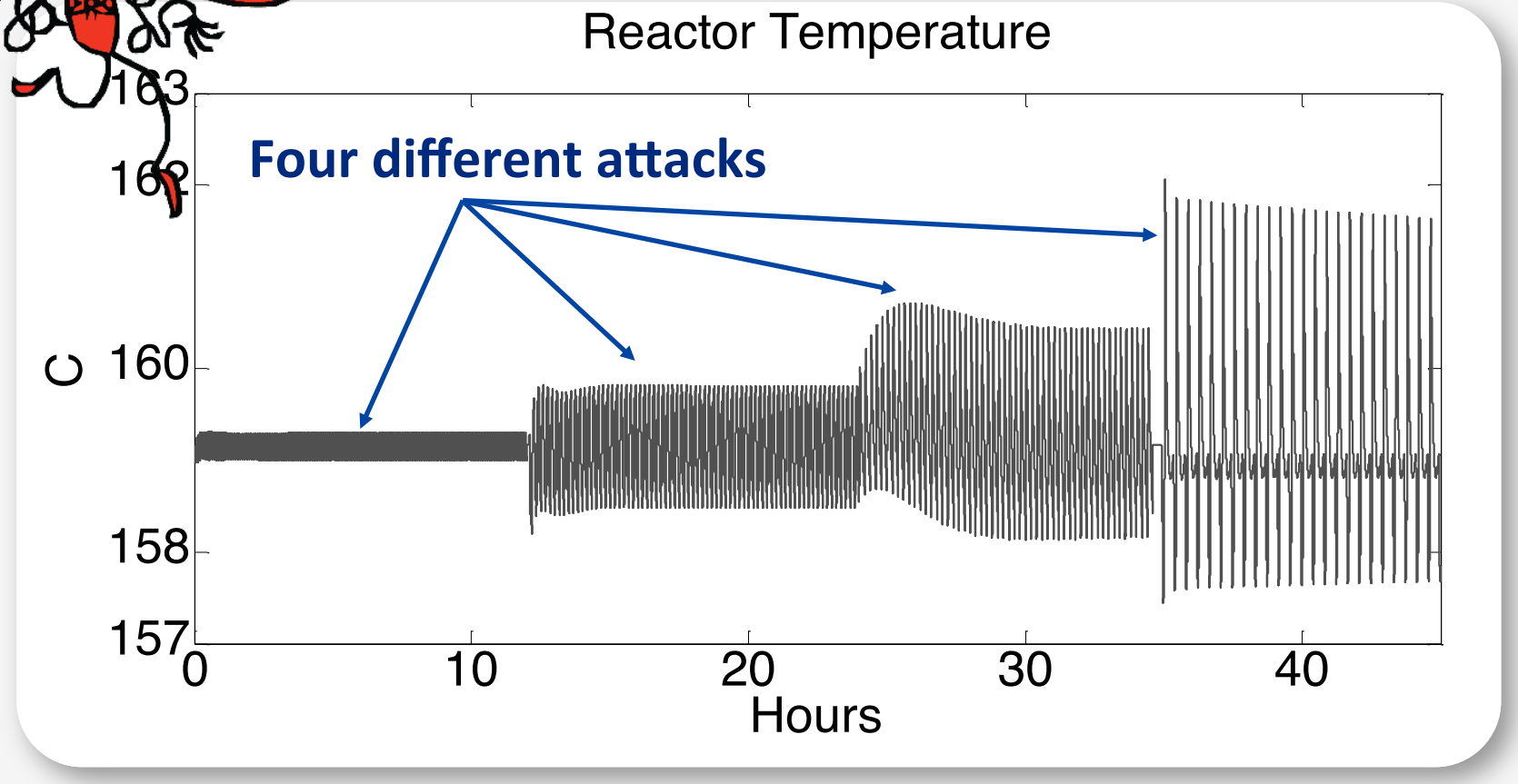
Creating forensics footprint

- Process operators may get concerned after noticing persistent decrease in production and may try to fix the problem
- If attacks are timed to a particular employee shift or maintenance work, plant employee will be investigated rather than the process

Creating forensics footprint

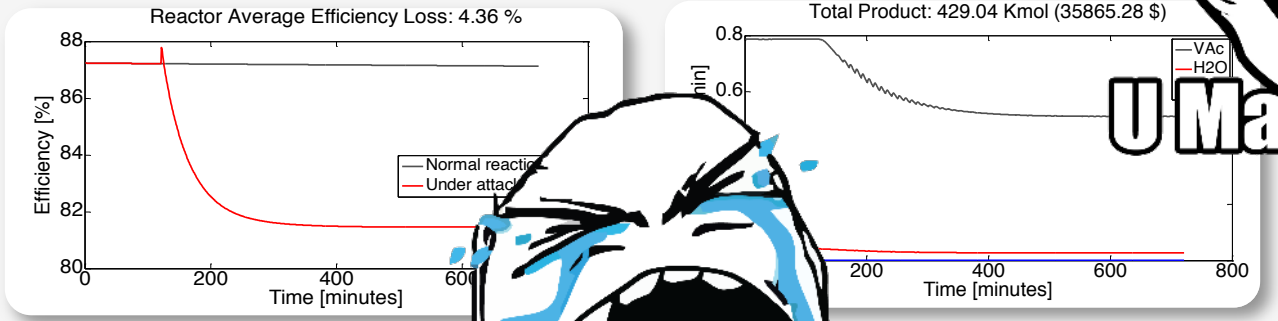
1. Pick several ways that the temperature can be increased
2. Wait for the scheduled instruments calibration
3. Perform the first attack
4. Wait for the maintenance guy being yelled at and recalibration to be repeated
5. Play next attack
6. Go to 4

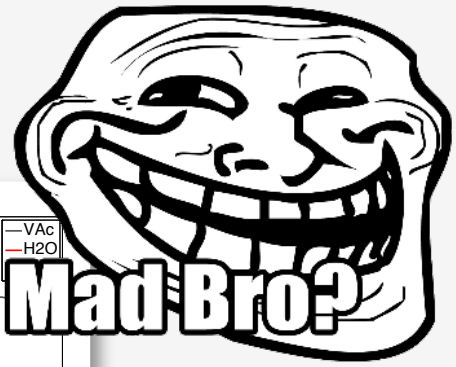
Creating forensics footprint



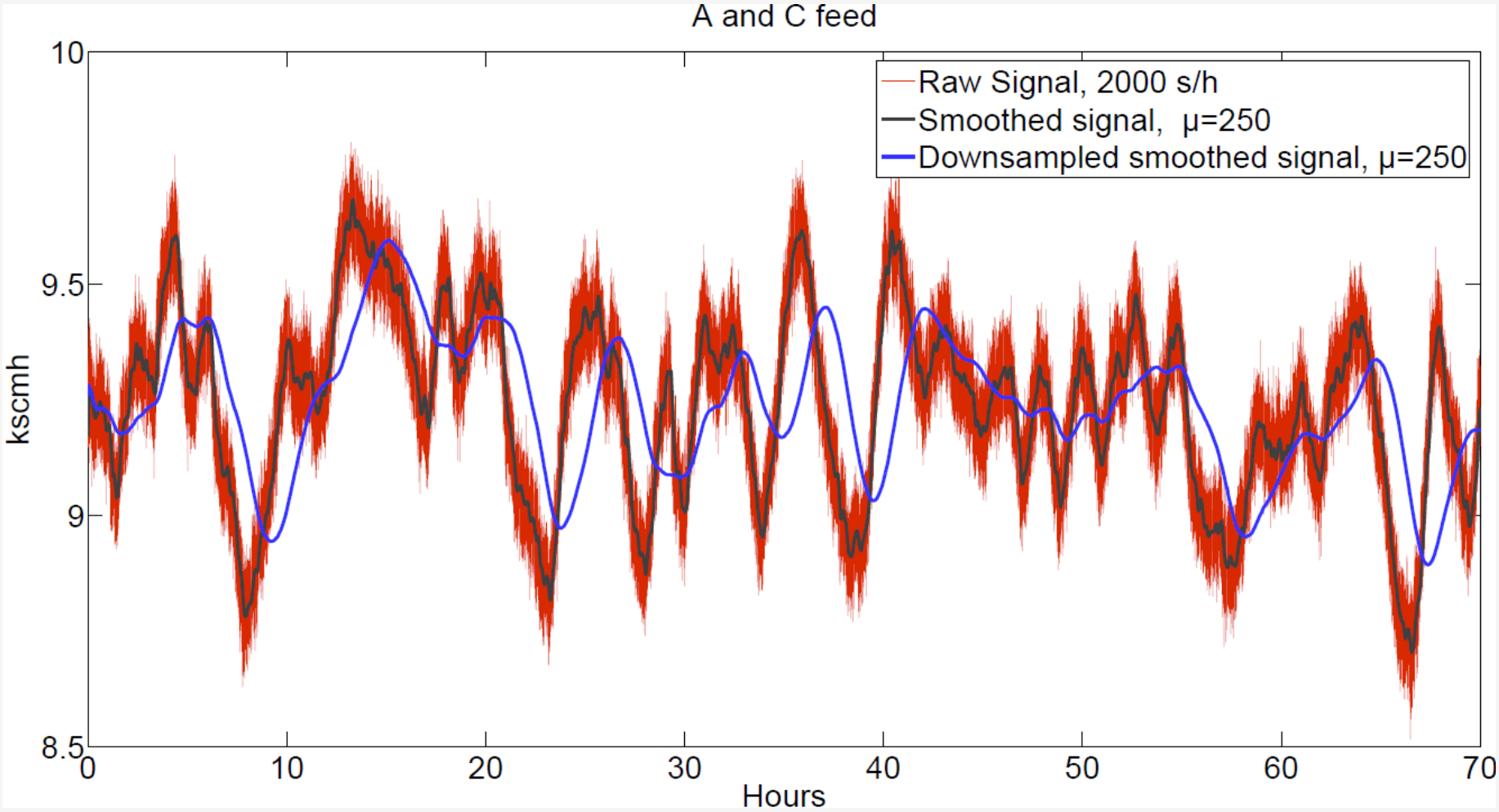
Defeating chemical forensics

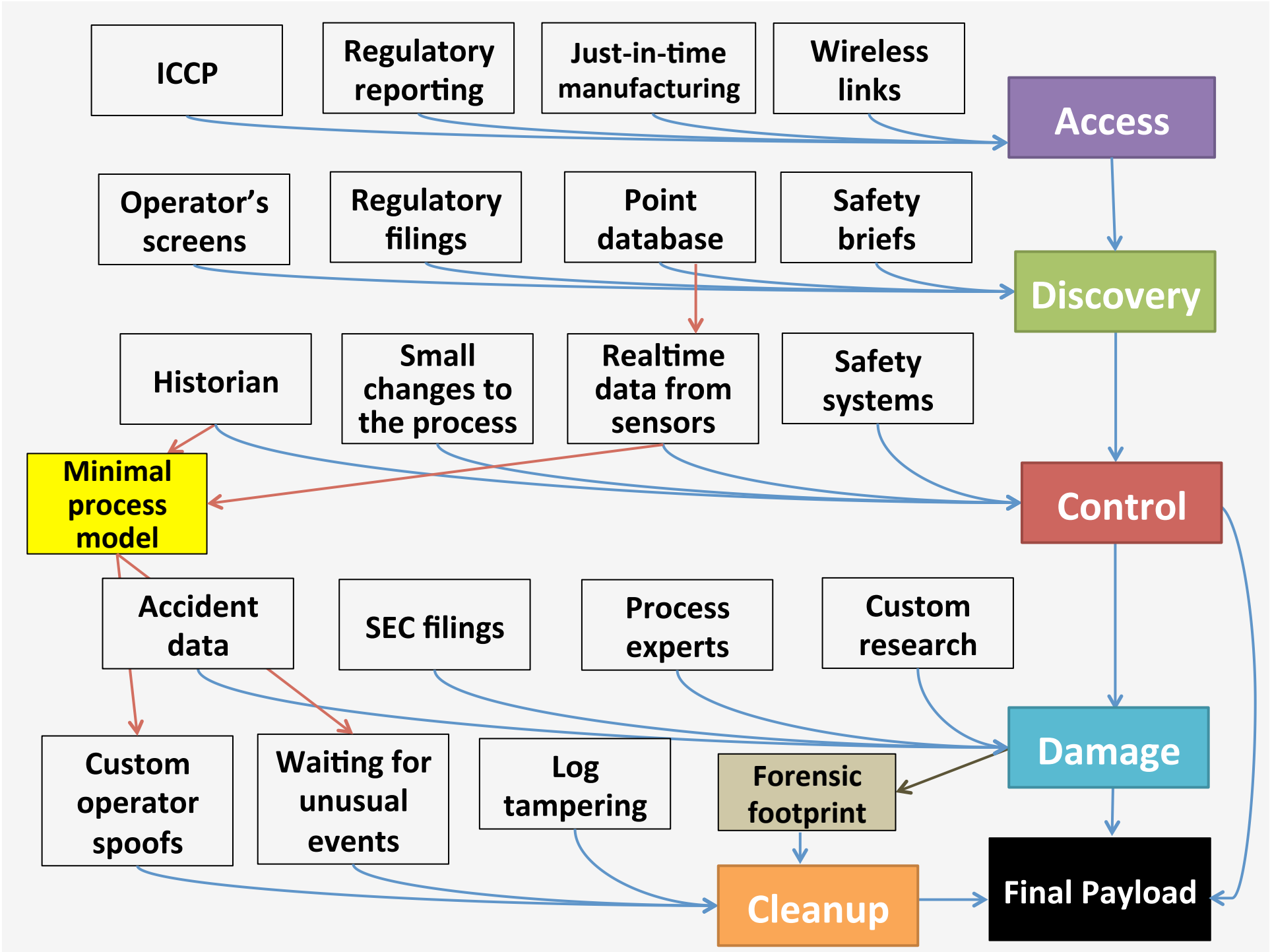
- If reactor deemed malfunctioning, chemical forensics will be asked to assist
- **Change attack patterns according to debugging efforts of plant personnel**





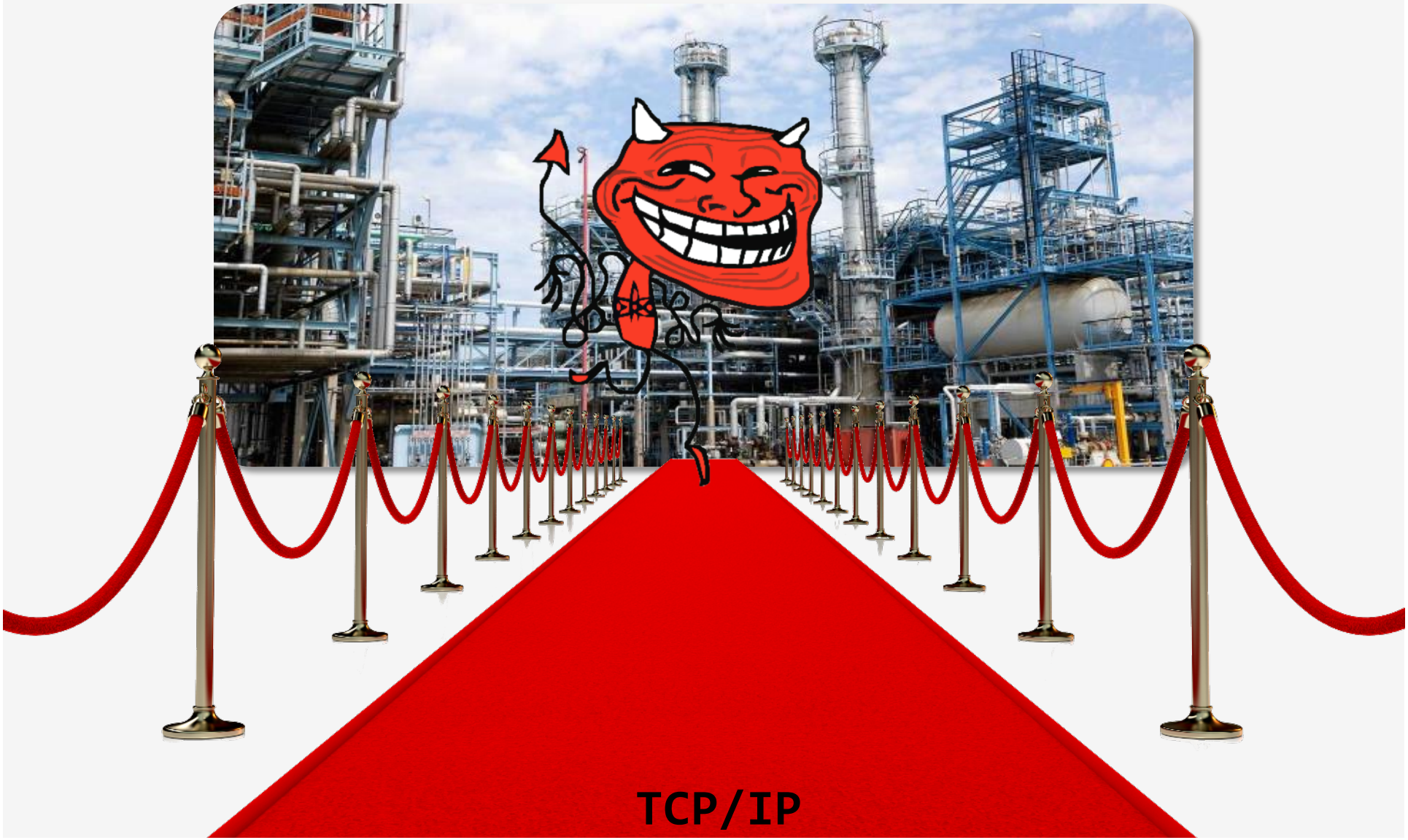
Data synchronization and processing




ICCP
Regulatory reporting
Just-in-time manufacturing
Wireless links
Access
Operator's screens
Regulatory filings
Point database
Safety briefs
Discovery
Historian
Small changes to the process
Realtime data from sensors
Safety systems
Minimal process model
Control
Accident data
SEC filings
Process experts
Custom research
Damage
Custom operator spoofs
Waiting for unusual events
Log tampering
Forensic footprint
Cleanup
Final Payload

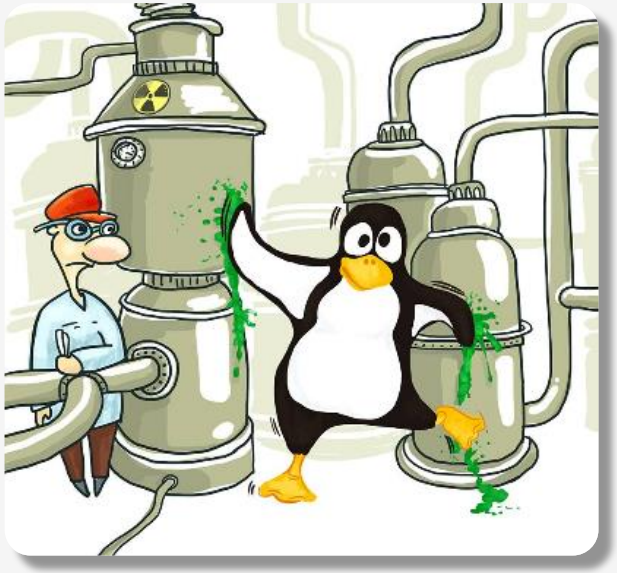
Afterword

State-of-the-art of ICS security



Food for thought

- **Cost of attack can quickly exceed cost of damage**
  - Hacking into large number of devices
  - Suppression of alarms and process data spoofing
  - Badly behaved control loops , synchronization of actions
- **Each process is unique, but…**
  - There are instances of attacks applicable to wide range of scenarios
  - **SCADA payloads for Metasploit is just a matter of time**



Thank you

marina.krotofil@tuhh.de

@marmusha

Damn Vulnerable Chemical Process

TE: http://github.com/satejnik/DVCP-TE
VAM: http://github.com/satejnik/DVCP-VAM

Thanksgiving:
Jason Larsen for all collaborations